



Cyber insurance

**Are insurers finding growth
or looking for trouble?**

2016

kpmg.com/us/insurance







Contents

Addressing the unmet need	2
Business value hinges upon managing cybersecurity	4
The current state of the industry and where it is heading	6
Despite the uncertainty, a market opportunity exists for insurers – but beware	8
Quantifying cyber risk	9
Where can insurers begin?	10



Addressing the unmet need

With cyber attacks considered “the biggest risk that global businesses are unprepared for,”¹ offering more and broader customized cyber insurance coverage may also represent one of the most promising growth products for insurance companies in quite a while.

Even with businesses of all sizes, across the spectrum of industries planning to increase spending on cybersecurity technology, services, and cyber insurance, insurers find themselves in a “go-slow” mode.

A number of cybersecurity issues emerged in KPMG’s U.S. CEO Outlook Survey. Here are four key findings:

- Two-thirds (66 percent) said they were only “somewhat prepared for a cyber event.”
- Half (51 percent) identified cybersecurity as the risk they are most concerned about.
- Nearly 4 in 10 (39 percent) said minimizing cyber risk is their top strategic priority for the next 3 years.
- And 37 percent said their top area of investment is cybersecurity solutions.

Understanding cyber risk by insureds and insurance companies alike is proving to be an enormous challenge. For some industry observers, gauging the attendant risks—at least for the moment—often amount to sheer guesswork where they are estimating the scope and impact of exposure.

¹ “A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity,” Allianz Global Corporate & Specialty SE, September 2015

The reasons for uncertainty and trepidation are varied and related: Insurers are finding it difficult to price cyber insurance, primarily because loss exposures are difficult to calculate due to a relative lack of data on the extent of losses. Due to the rapidly evolving nature of these risks, insurers are finding it difficult to keep up. Further, there is a paucity of experienced insurance personnel with cyber insurance background.

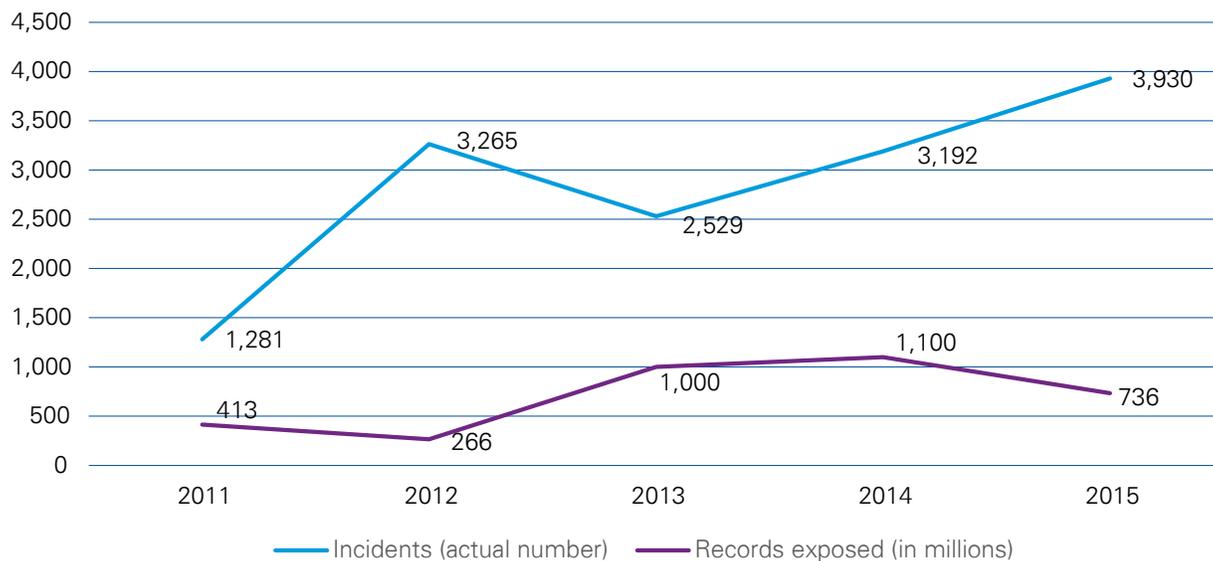
Aside from concerns about understanding cyber coverage issues, our research indicates that cyber attacks on insurance businesses are also a major concern.

In this crucial moment, progress must be made in gathering, modeling, and interpreting cyber risk and cybersecurity data. Without analytical advances, insurance companies can expect to struggle in helping potential business clients assess vulnerabilities in coverage gaps. What’s more, insurers themselves would be at a

disadvantage in their need to create sound pricing and set aside proper loss-reserve amounts. Such a scenario could surely invite regulatory scrutiny and negatively impact reputation.

“ A central issue we see right now in the industry is that the data on which so many pricing and reserving decisions must be made is either not readily available, or it is disjointed,” said Laura Hay, national sector leader of the KPMG Insurance practice. “Having that data—along with the comfort that it is high-quality data—is essential if insurers want to create accurate models and come to well-informed decisions. ”

Data-breach trends



Source: “2015 Reported Data Breaches Surpasses All Previous Years,” Risk Based Security.

Business value hinges upon managing cybersecurity

Protecting businesses against cyber attacks goes well beyond safeguarding data and network: It is an issue central to reputation and regulatory compliance, and it enables businesses to continue financial stability while possibly avoiding damaging litigation. **(See chart: “What are your top concerns in a breach” from KPMG’s 2016 Consumer Loss Barometer)**

“Forbes Insights and KPMG surveys of 403 corporate executives and 750 consumers provide deeper understanding of how cybersecurity management—

or mismanagement—can create or destroy value.”² The risks to many organizations are varied, as illustrated in the survey finding (below) that is included in the 2016 Consumer Loss Barometer.

“*In too many industries, information security is still seen as a technology risk to be minimized instead of a business issue to be optimized.*”
 — Greg Bell, U.S. Leader, KPMG Cyber

What are your top concerns in a breach?

The risks are many and costly to both the organization’s stature and bottom line.

Overall



Financial services



Tech



Retail



Automotive



KPMG Consumer Loss Barometer.³

² KPMG Consumer Loss Barometer, July 27, 2016

³ Ibid

You need to prioritize your most important assets—your crown jewels—as you consider your sensitive data.



Sensitive data

KPMG Cyber's view by category

Changing targets

Data category

An important part of a cyber approach is identifying what data is sensitive and critical to each stakeholder in the information life cycle. This categorization of data helps drive a risk-based cyber agenda and meaningful investment.

Corporate



Intellectual property, Research, Development, Mergers, Acquisitions, Divestitures, Trade secrets

Customer



Patients, Benefits, Financial, Health

Employee



Human resources, Payroll, Health, Benefits, Performance reviews

Third party



Commercial agreements, Rate cards, Hosted data, Managed data

Attorney-client



Lawsuit, Arbitration, Privileged communications

The current state of the industry and where it's heading

Advancing numbers of data breaches, driven by massive digitization of business processes and mobile computing, has resulted in huge security spending. In KPMG LLP's (KPMG) recently published CEO Survey, respondents reported that finding a solution to cybersecurity issues is their top priority during the next three years.

In 2016, spending for cybersecurity products and services is expected to reach \$60 billion, and IT security spending could reach \$100 billion by 2018, with the potential to climb to \$170 billion by the end of the decade.⁴ Spending on security technology alone cannot and will not help solve cybersecurity challenges. Solutions should be supported by strong process information sharing among the industry and strong leadership with board oversight.

Annual losses attributable to cyber crime is approaching \$500 billion, according to research from Allianz.⁵ And Juniper Research predicts "rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to \$2.1 trillion globally by 2019."⁶

Yet for all the hype about its need and its potential to assist insurers and the insured, cyber insurance commercial premiums are the proverbial drop in the bucket—cyber premiums represent a fraction of 1 percent of global commercial insurance premiums.⁷ Analysts at Aite Group LLC predict that "...for the foreseeable future, the insurance industry will be marketing a product that raises expectations, but that few truly understand."⁸

The analyst community has indicated that cyber insurance buyers, who must comply with the increasing number of data privacy breach-notification laws, are not satisfied with the availability and the coverage limits of current offerings. The reasons are varied: There are restrictions on coverage, some (perhaps many) policies are difficult to understand, claims can be difficult to determine, and litigation issues often cloud the process.

"Unfortunately, more security doesn't necessarily mean better security. In fact, the current strategy of most organizations—layering on many different technologies—is not only proving ineffective, it is overly complex and expensive. The status quo is not sustainable," says Keith Weiss, head of U.S. software coverage for Morgan Stanley. "Even as companies spend more on security, losses related to cyber crime have nearly doubled in the last five years."

Excerpt from "Cybersecurity: Time for a Paradigm Shift," Morgan Stanley, June 15, 2016



⁴ "Worldwide Cybersecurity Spending Increasing To \$170 Billion by 2020," *Forbes* magazine, March 9, 2016

⁵ "A Guide to Cyber Risk," Allianz, September 2015

⁶ "Worldwide Cybersecurity Spending Increasing To \$170 Billion by 2020," *Forbes* magazine, March 9, 2016

⁷ "Cyber Insurance and Cybersecurity: The Convergence," Aite Group LLC, June 2016

⁸ *Ibid*

Simply put, a cyber breach would almost certainly lead to compromise in several areas, according to Jim Wilhelm, a KPMG Advisory managing director in the firm's Information Protection practice.

In terms of confidentiality, a breach could lead to loss of company information, either intellectual property or consumer information, leading to potential regulatory fines, reputation loss, and/or competitive advantage.

There would almost certainly be a negative impact on network integrity, specifically as it relates to the reliability of information and information systems, as well as possible business interruption incidents and reputation damage.

Moreover, a breach may have a negative impact on availability, including the accessibility of computing assets, customer impact, business interruption, and other fundamental business areas.



“Availability of broad coverage isn't going to happen overnight,” said Carl Groth, a KPMG Advisory managing director in Actuarial and Insurance Risk. “Many of the businesses that want to increase offerings are ramping up quickly. But it is important for these insurance businesses to be certain that they are using accurate methods to forecast losses, making sound decisions on pricing, and employing a very reliable method to allocate the proper level of risk capital in the event of a major loss event.”



Despite the uncertainty, a market opportunity exists for insurers – but beware

In a recent interview with KPMG, James Auden, managing director at Fitch Ratings, discussed a March 2016 report Fitch published on insurers offering more cyber coverage.

Auden said the ratings agency “would view aggressive growth in stand-alone cyber coverage, or movement to high portfolio concentration in cyber, as ratings negatives.”

He said cyber insurance “is a very new product, relatively speaking. There is a real need in the marketplace, and it is growing. And, insurers have a unique set of skills and capabilities to help meet those needs—more so, for example, than technology firms. Insurers are particularly equipped for risk management and for processing or remediating claims.”

He added that while offering cyber coverage “is a potentially very good opportunity for insurers...there are a lot of perils with the new product. There isn’t a lot of claims information or history, when compared to other insured events, to rely on, so that makes pricing difficult.”

Further, Auden said, “In terms of framing and shaping the coverage...we do see further events that are cyber-related, and insurers could have a lot of exposure, and there could be considerable losses. So, that is really our concern—that some insurers will write a business that they don’t fully understand... An insurance company could be really harmed if it didn’t know what it is fully getting into.”

The Fitch report stated: “Underwriting, pricing, and reserving uncertainties currently outweigh the potential earnings growth benefits. Controlled growth as part of a diversified portfolio, coupled with continually enhanced underwriting standards, would generally be neutral to ratings.”

Source: “Expanding Threats Amplify Underwriting Opportunity, Loss Potential,” Fitch Ratings, March 21, 2016)

In less than 10 years, global cyber insurance premiums will reach \$20 billion, an increase of more than 10 times the current level, according to Allianz.⁹

Yet, currently, only fewer than half (40 percent) of FORTUNE 500 companies have insurance against cyber incidents, and like many other businesses, most of those who have purchased the insurance have coverage with limits that do not cover the entire cyber exposure.¹⁰

However, even if insurers seek to offer more cyber coverage, they may first be interested in considering a recent comment by a Fitch Ratings analyst, (see left side bar) who suggested that any aggressive entry by an insurer into the market may carry a downside risk.

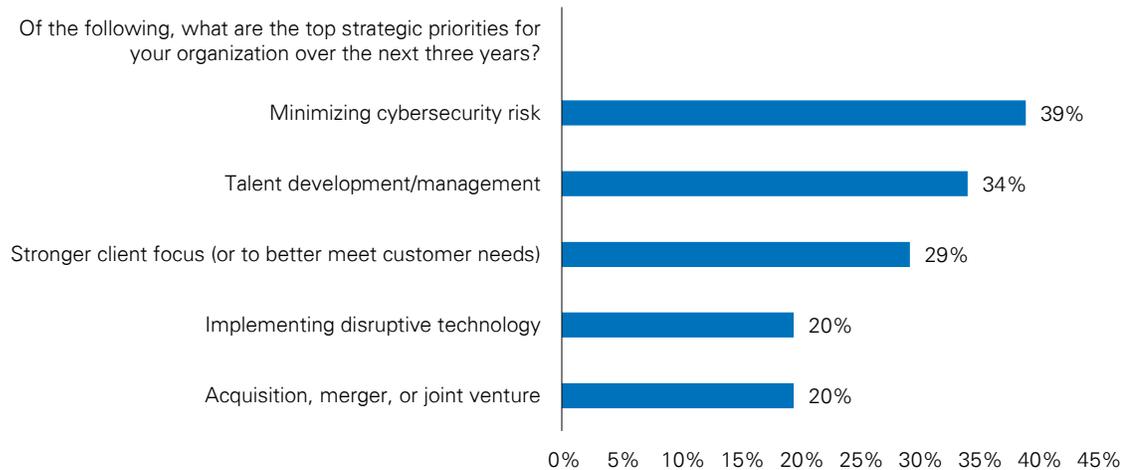
⁹ “Cyber risk 2025 – The next 10 years,” Allianz, July 2016

¹⁰ “Can startups disrupt the \$20 billion cyber insurance market?,” TechCrunch, May 23, 2016

Quantifying cyber risk

One of the key findings of KPMG's recent U.S. CEO Outlook Survey dealt with prioritizing strategic risk: It comes as no surprise that cyber is at the top.

Top strategic priorities for the next three years

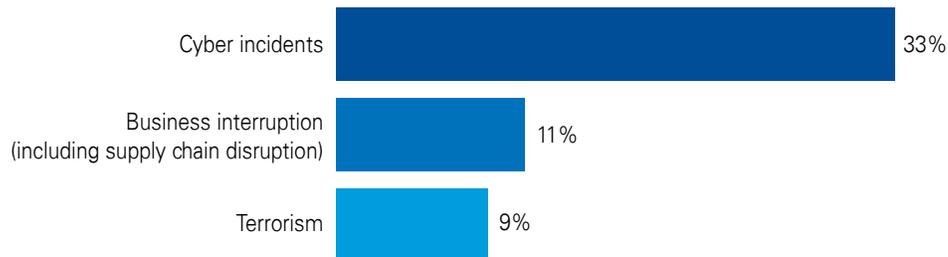


Source: KPMG's 2016 Insurance Industry CEO Outlook Survey

Further, according to the Allianz 2016 Risk Barometer, which polled 800 risk managers in 40 countries, cyber incidents are considered the top emerging risk for the long-term future.

Even though business customers are eager to buy coverage, many have a limited understanding of their organizations' risk factors. According to a NetDiligence 2015 Cyber Claims Study, 48 percent said they had little appreciation of the complexity of the cyber risks their businesses faced.

What are the top emerging risks for the long-term future (10+ years)



Where can insurers begin?

KPMG's five practical ideas for carriers evaluating the cyber insurance opportunity

Ideas for future growth start with deliberate consideration of scenarios and questions regarding where an organization is positioned on the path toward growth.

Here are our five steps for consideration. They are rooted in our belief that cyber insurance has a future for organizations that are willing to take calculated risks and that would consider seeking assistance or alliances where it is sensible or necessary.



Ensure that writing cyber risk coverage fits into the company's overall strategy.



Organize teams that can determine your customers' (and potential customers') cyber risk profile.



Create specific areas of examination in order to understand an insurer's control environment.



Consider where the best sources of data and other information exist in order to price coverage properly.



Use your senior-level team for making decisions about the aspects of cyber risk coverage to provide to the market.



Ensure that writing cyber risk coverage fits into the company's overall strategy.

Using senior-level operational and strategy management members, along with board members who have background in risk management, convene specific meetings for the purpose of determining whether cyber risk coverage fits into the insurer's business strategy:

- Essential focal points in the discussions will be to understand whether underwriting cyber coverage will grow the top line, improve the overall "customer experience," and enhance returns on risk capital.
- The exploratory team should ask this question: Is our decision to underwrite this coverage made with a long-term view on how our risk profile might change in an increasingly competitive environment?



Organize teams that can determine your customers' (and potential customers') cyber risk profile.

Understanding an insured's cyber risk profile is essential, but that task is increasingly difficult to perform because of the rapid increases in the number of attacks and the changes in cyber threat vectors. Nevertheless, it is a vital undertaking in order for carriers to be able to price coverage properly and make decisions on whether to offer cyber insurance coverage:

- Think of the ways business is conducted now compared to just a few years ago and then consider the changes in a business's cyber risk profile: cloud computing, big data, social media, mobile computing, robotic process administration, cognitive/machine learning, and the Internet of Things. Have your insurance risk considerations kept pace?
- Moreover, technological change is accelerating at exponential speed, potentially creating severe IT infrastructure inefficiencies. Gap analyses regarding inefficiencies are fundamental in creating a company's risk profile. However, gap analyses are only the beginning.



Create specific areas of examination in order to understand an insurer's control environment.

Begin by interviewing the business's risk governance personnel and seek to understand whether the organization has included specific cybersecurity measures in its risk governance framework:

- Have any recent tests that seek to reveal any "black holes" in the effectiveness of the insureds' control environment been performed? If not, ask why not and when one is planned.
- Take the company through threat assessments, cybersecurity assessments, penetration testing, and other assessments in order to create a potential "win-win" proposition to help the business better understand its cyber risk control environment. The information gained can help insurers improve their ability to appropriately structure and price cyber coverage.



Consider where the best sources of data and other information exist in order to price coverage properly.

Although the amount of cyber loss information continues to increase, there are data and information challenges associated with pricing the coverage due to the rapidly changing nature of the underlying exposure and threat vectors:

- Consider teaming with third parties in order to obtain valuable information to help with pricing.
- Create internal teams that can evaluate the assessment and testing services of third parties that might help with this complex data challenge.
- Look for organizations, or internal personnel, with experience in building pricing models and incorporate that data to get comfortable with pricing.
- Consider using backtesting as a tool to ensure the adequacy of pricing methodologies, given the rapid changes in exposures over time.
- Make certain of understanding the insurance company's capability to provide these services compared to partnering with vendors.
- If considering using a vendor, due diligence about vendor capabilities is critical. Seek internal and external guidance in creating evaluation criteria.



Use your senior-level team for making decisions about the aspects of cyber risk coverage to provide to the market.

There is almost an endless number of potential policy features and coverage characteristics. Wading through the options can be challenging, particularly for an insurer thinking about entering the cyber insurance market:

- Decide which coverage characteristics make sense to be offered in the market, given pricing challenges and the potential for an increase in market participants/competition.
- Be certain that the team assesses issues, such as coverage triggers, discovery periods, extortion coverage, changes in control, digital asset replacement coverage, reputational injury coverage, breach response capabilities, litigation management, and the many other issues that should be addressed for potential inclusion in the policy design.
- Focus on how your insurance company's cyber policy dovetails with other coverages that are provided. Create a process to collect and analyze market intelligence on competitors' products and related price points and pricing trends.
- Given the range of outcomes, be sure to understand the services that the insurance company can offer to contain losses for customers and the insurer.

Aon's Cyber chief: Insurers are treading ahead cautiously

When it comes to thwarting cyber attacks on businesses across industries, the bad guys are still far ahead of the good guys.

The rub, of course, is that, as massive data and financial losses, reputation damage, and business interruption events keep mounting, many businesses are in the position of being underinsured relative to the risks involved.

"Cyber coverage is evolving and maturing, but the threat environment is changing much faster," says Christian Hoffman, national practice leader at Aon's, Professional Risk Solutions. "The result is that insurers are still trying to gain comfort around the scope of the losses, the data, and the ability to model in order to properly underwrite and protect both clients and themselves."

"We need more large, tier-one insurers offering this risk protection at a primary level," Hoffman adds. "But, essentially, we are talking about a four-year-old frequency issue. That has meant insurers being understandably cautious about offering cyber insurance from a primary perspective, especially coverage such as the type that covers business interruption."

Like others in the industry, Hoffman says he expects insurers to continue to form partnerships with third parties in order to enhance their data modeling capabilities and eventually offer more coverage and broader terms.

While the marketplace for cyber insurance continues to develop, there are fears in the investment community that insurers could be tempted to move too quickly as they pursue growth opportunities. Fitch Ratings has already issued a client memorandum (see the sidebar on page 7) to investors, suggesting it could impose lower ratings on insurers that pursue cyber insurance underwriting too aggressively.

A fundamental first step for any business is to view cyber risk as much more than a technology concern. "That's just a piece of the puzzle; cyber is an enterprise issue. There is a long list of constituents, starting with the board of directors, who need to help the business understand the risks in order to prepare on the front end and then manage the incident when it happens," Hoffman says.

With regard to cyber insurance, the risk manager must be in constant contact with the general counsel, the information security team, and the finance team to review coverage and prepare a cost-benefit analysis. In order to empower employees to be more informed and vigilant on cybersecurity-related issues, human resources leaders must be involved to implement more in-depth training programs.

Aon itself has quickly responded to the growing demand for cyber insurance: "In the past two months, we have added 10 colleagues, increasing the team from 40 to 50 people. Compared to 2 years ago, we are now double the size. If you looked at us in 2010, we had no cyber expertise in our New York office. We now have 12 dedicated colleagues."

About the authors



Laura Hay

ljhay@kpmg.com
212-872-3383

Laura is a principal in KPMG's Insurance practice and serves as the national sector leader for Insurance. She has more than 30 years of professional experience in the insurance industry, focused on audit, advisory, and actuarial services. She was named to *Consulting* magazine's *Women Leaders in Consulting List* in 2012. Laura is a member of the American Academy of Actuaries and a Fellow in the Society of Actuaries.



Jim Wilhelm

jameswilhelm@kpmg.com
267-256-7271

Jim is a managing director in KPMG's Cybersecurity practice, with more than 12 years of experience providing information security and identity and access management assistance to clients across a variety of industry verticals.

During his time at KPMG, he has served as a member of our leadership team with responsibility for business development and execution of IT risk and security services, including identity management planning, implementation, and strategic security program transformation initiatives.

Contributors:



Ali Geramian

ageramian@kpmg.com
202-533-3642

Ali is a member of KPMG's Innovation Lab, which focuses on sensing and understanding signals of change through a people-first lens. Leveraging design thinking and an outside-in perspective, members of KPMG's Innovation Lab help identify how those signals may impact the growth and relevance of organizations based on their decade of research and knowledge in neuroscience and human creativity, as well as leadership in technology innovation, trends analysis, and start-up scanning.

About KPMG's Insurance practice

Insurance markets face a wide range of complex challenges today, from navigating financial market uncertainty and evolving consumer demands to new technologies and the need to outpace digitally smart new competitors. These forces may demand swift action to outmaneuver immediate concerns. Or, they may require a gradual evolution of strategy to incubate potential opportunities.

At KPMG, our network of experienced professionals understand these changes. We know what it takes to turn disruption into advantage in order to help insurers thrive in a changing world. Our multidisciplinary teams combine deep industry experience with specialist knowledge to deliver tailored, value-added solutions.

In a constantly changing business, economic and regulatory environment, we put our clients at the center of our thinking, providing integrated approaches that help them create and protect value, mitigate risk, and uncover opportunities in times of change.

Contact us:



Laura J. Hay
**National Sector Leader,
Insurance**
T: 212-872-3383
E: ljhay@kpmg.com



Matt McCorry
**National Advisory Leader,
Insurance**
T: 212-954-3945
E: memccorry@kpmg.com

kpmg.com/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstance of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 599188