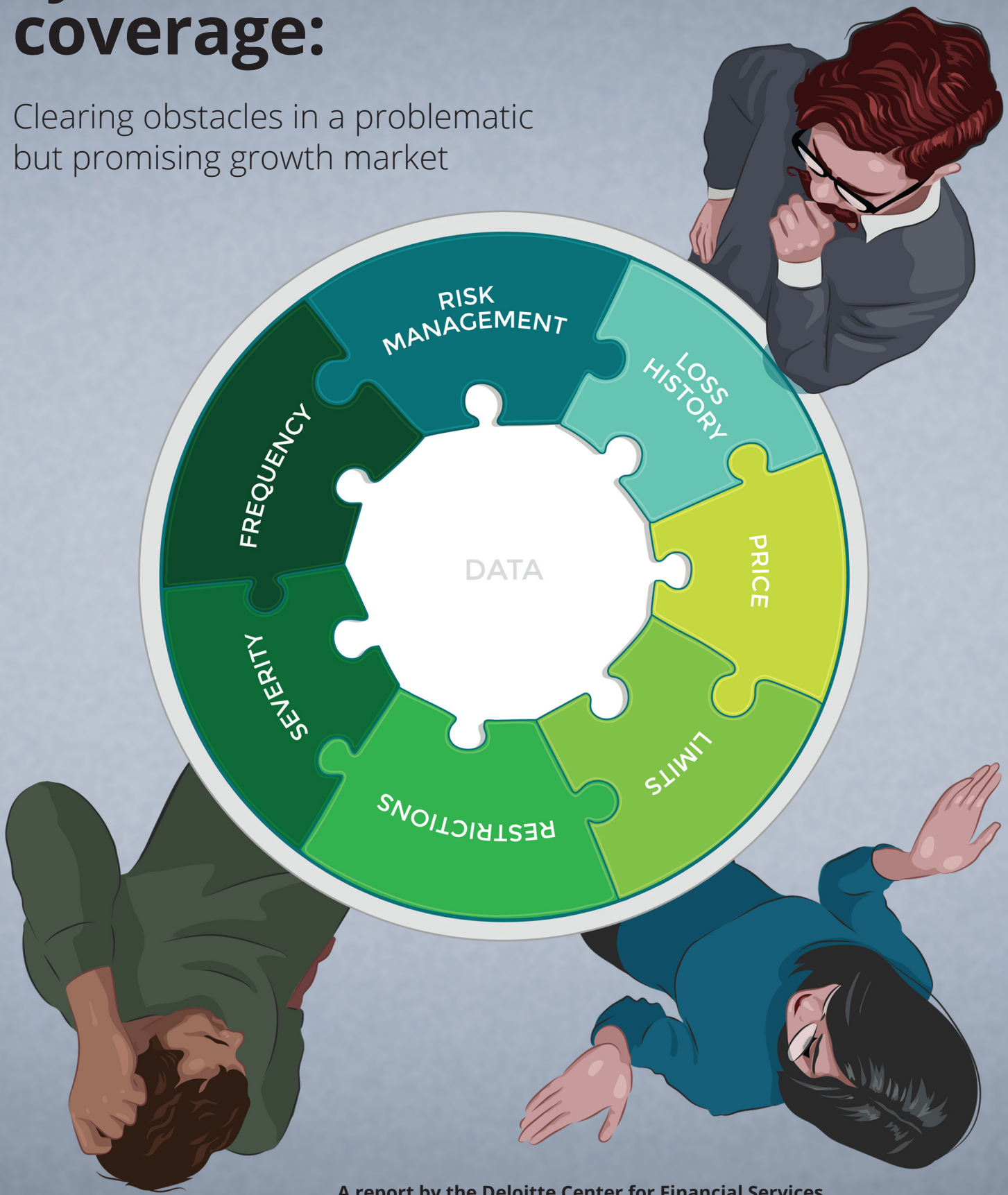
Demystifying cyber insurance coverage:

Clearing obstacles in a problematic but promising growth market

Deloitte. University Press



A report by the Deloitte Center for Financial Services

About the Deloitte Center for Financial Services

The Deloitte Center for Financial Services, part of the firm's US financial services practice, is a source of up-to-the-minute insights on the most important issues facing senior-level decision makers within banks, capital markets firms, mutual fund companies, investment management firms, insurance carriers, and real estate organizations.

We offer an integrated view of financial services issues, delivered through a mix of research, industry events, roundtables, and provocative thought leadership—all tailored to specific organizational roles and functions.

CONTENTS

Cracking the code on cyber insurance

With most US property and casualty insurers struggling to grow in a slowly recovering economy, an overcapitalized market, and a historically low interest-rate environment, why isn't the sale of cyber insurance gaining momentum more quickly, given the rising profile of the risk?

THE line still only generates between $1.5 billion and $3 billion in annual US premiums thus far, according to various industry estimates by regulators and rating agencies—representing only a tiny fraction of the $505.8 billion[1] domestic carriers wrote in total in 2015.

Yet despite that rather modest starting point, a number of industry leaders are bullish about the cyber market's future. Some are predicting US sales to double or even triple over the next few years, according to the Insurance Information Institute.[2] Allianz Global Corporate & Specialty foresees a worldwide market of more than $20 billion by 2025.[3]

The industry has a long way to go to reach those lofty predictions. Many commercial enterprises have yet to purchase a cyber policy—or if they have, their coverage tends to leave them underinsured. Just 29 percent of US businesses had bought cyber insurance as of October 2016, according to a survey by the Council of Insurance Agents and Brokers (CIAB).[4] While bigger companies are more likely to buy the coverage, the majority of large organizations are still going bare on the exposure. Indeed, a September 2015 CIAB study found only 40 percent of Fortune 500 companies had cyber insurance at that time, while those that did often bought limits that didn't cover the full extent of their exposure.[5]

Therefore, conditions seem ripe for cyber insurance sales to take off, especially since consumer awareness of the exposure appears to be on the rise. This is thanks, in part, to the proliferation of widely publicized breaches in the private and public sectors, and as more individuals fall victim to identity theft.[6] So, with a potentially huge exposure gap for the industry to fill, why have insurers generally remained cautious about writing cyber coverage on a large-scale basis? And why are so many prospects still hesitant to add the coverage to their insurance portfolios?

What circumstances might prompt insurers to do more than dip their proverbial toes in this growing risk pool? And what steps could the industry take to help prospective buyers large and small better understand their cyber risks and the role insurance could play in protecting them? To generate ideas that would address both these questions, the Deloitte Center for Financial Services reviewed secondary research and spoke with a variety of industry players. These conversations included a pair of primary carriers writing the coverage (one in the United States and the other in Europe), as well as a trio of brokers buying coverage for cyber risks globally in the commercial, specialty, and reinsurance markets. We also collaborated with Deloitte's Cyber Risk Services practice to harvest the lessons learned from their work helping insurers resolve many of the industry's underwriting and pricing conundrums.

Our research revealed a number of significant obstacles carriers face when contemplating the sale

Figure 1. Obstacles to meeting demand for cyber coverage

Insurer's perspective	Consumer's perspective
• Dearth of data • Cyber attacks keep evolving • Potential catastrophic accumulation • Tunnel vision in coverages offered	• Buyers often don't understand cyber risks or their insurance options • Cyber risk is spread over a wide range of coverages • Cyber policies lack standardization • The legal landscape remains in flux

Source: Deloitte Center for Financial Services.

of cyber insurance, as well as issues causing many prospects to hesitate when considering a transfer of at least a portion of their risk to third parties (see figure 1).

Insurers will likely need to overcome these obstacles to fully realize the upside potential of this problematic yet promising market. At the moment, cyber insurance remains a work in progress when it comes to assessing the risks carriers face and providing a clear, comprehensive, and high-value set of products and services to attract more buyers into the fold. However, there appear to be opportunities for insurers to adjust their strategies and operations to reach, and perhaps even surpass, the growth rates anticipated by various industry prognosticators—and, most importantly, to do so profitably.

In this article, we'll explore the roadblocks hindering the market's growth as well as how these hurdles might be cleared. And as a cautionary tale, we'll point out that those who hesitate may indeed be lost when it comes to selling cyber insurance. Alternative risk-transfer vehicles such as captives, risk retention groups, and insurance-linked securities may eventually limit insurer penetration, and perhaps even largely displace traditional carriers, if the industry doesn't soon crack the code and become a more reliable provider of adequate, understandable, and affordable cyber coverage.

Obstacles from the cyber insurer's perspective

Dearth of data leaves insurers in the dark

One prime reason why insurers have struggled to get their arms around cyber risk is the lack of historical data, which makes it difficult to build the predictive models that can help assess probability of loss. Hard data is in short supply for a variety of reasons, according to those we interviewed. One is that insurers have not been selling cyber insurance long enough or on a big enough scale to generate their own critical mass of data. There is also no comprehensive, centralized source of information about cyber events for insurers to tap into. In addition, a large percentage of cyber losses aren't even acknowledged to outsiders, as the Insurance Information Institute notes that "many, if not most, attacks go unreported and undetected."[7]

At the same time, the bulk of reported losses involves breaches that expose personally identifiable information (PII), often because of legal notification requirements in various states. Yet such claims likely do not cover the full gamut of cyber exposures faced by companies and their insurers. Other cyber events—such as denial of service attacks, ransomware, and theft of intellectual property—are often kept under wraps. Insurers should, therefore, take potential reporting bias into consideration when building predictive models as well as underwriting and pricing systems.

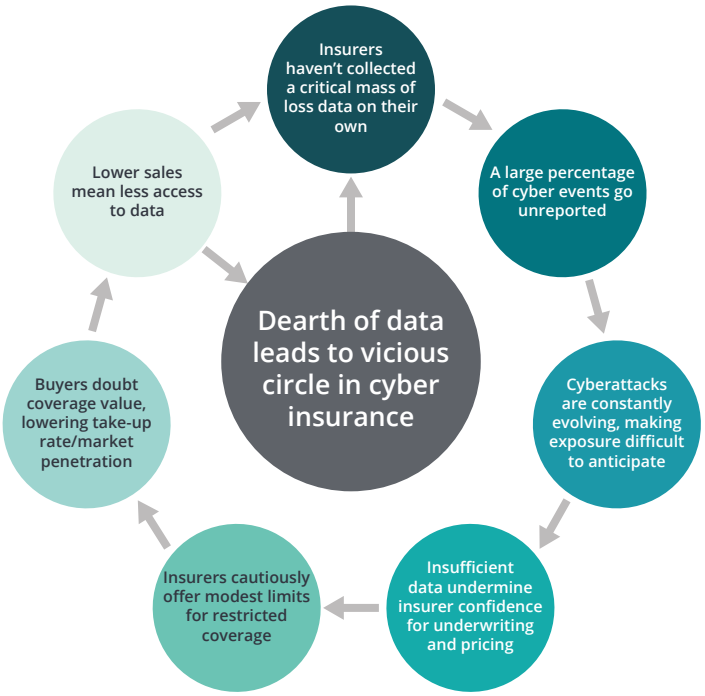
We believe this dearth of data may be producing a "vicious circle" of data-related obstacles hindering the growth of stand-alone cyber coverage in the high-end commercial market (see figure 2). First, insufficient data typically undermines insurer confidence in underwriting and pricing, which likely prompts carriers to play it safe by offering relatively modest limits and tightly restricted coverage. That can lead buyers to question the value of the coverage being offered for the premiums charged, which may inhibit sales and undermine market penetration. That would undercut the amount of primary data insurers can collect to more knowledgeably price exposures. This likely discourages them from writing more expansive coverage, which, in turn, would depress sales—starting the circle all over again.

Cyberattacks continually evolve, while new risks keep emerging

Another challenge facing cyber insurers of all stripes is the inherent volatility of this ever-evolving risk, which limits the value of historical experience and undermines the exposure's predictability. Existing cyber exposures keep mutating, while new ones are continually arising. Chief information security officers (CISOs) at insurance companies, banks, and investment institutions interviewed for a cybersecurity study by the Deloitte Center for Financial Services reported that as they adapt to one type of attack, threat actors keep coming up with new techniques, targets, and points of entry to exploit, making risk management an ongoing predicament.[8]

Those we spoke with for this report pointed out that even as insurers collect more data and hone predictive models based on prior cyberthreats, the underlying exposure keeps changing. It's therefore difficult to create a reliable predictive model when it's not clear what new objective, strategy, or technique hackers may come up with next. Insurers simply don't know what they don't know when it comes to cyber risks.

Figure 2. The vicious circle of cyber insurance



Source: Deloitte Center for Financial Services.

"We're trying to keep pace with the cybersecurity market, but the exposure is evolving in terms of what threat actors will do and what they are capable of, and as a result, it's very difficult to anticipate what kinds of attacks they will use and methods they will employ," noted one insurer we interviewed.

Complicating matters is that the operational landscape is also in flux. As insurers struggle to measure and model current risks, some are concerned about whether the industry will be able to keep up with any new cyber exposures that may emerge, such as those generated by the proliferating Internet of Things (IoT) and the development of autonomous vehicles. Such advances create new cyberattack possibilities to be assessed, detected, mitigated, and insured. While this certainly provides new opportunities for cyber insurers, it also generates a plethora of additional hazards to consider without much—if any—historical data to frame them.

Insurers fear potential catastrophic accumulation of cyber exposure

Many cyber insurers are concerned about biting off more risk than they can chew, let alone swallow. Besides the considerable challenge of underwriting and pricing cyber exposures given the dearth of data cited above, insurers may fear being overwhelmed by a sudden aggregation of losses.

One of the insurers we spoke with wondered what would happen "if tomorrow a website host is hit with a denial of service attack or is hacked. What if they're unable to service their clients? All those who have their websites on that platform might not be able to do online business while the third-party server is offline. There's a real aggregation risk there. How do we know whether our cyber insureds aren't all in one basket—cloud, website host, e-mail server, software-as-a-shared service?"

While such third-party facilities and vendors could very well have their own cyber policies in place, it's not clear if that would provide adequate coverage for losses suffered by their individual clients, who, as a result, would likely need their own insurance protection to deal with the fallout of a systemic event.

Brokers placing business in the market told us that reinsurers in particular seem skittish about the potential for a "cascading" event triggering a wide range of policies across companies, countries, and entire industries. Some brokers fear that a lack of significant reinsurance support may create another drag on growth, keeping the cyber market from taking off.

A number of those we interviewed cited comparisons with the terrorism insurance market. Terrorism risks are akin to cyber exposures because both involve human actors intentionally looking to harm insureds, and in that such attacks can occur anytime, anywhere, to virtually anyone (unlike natural catastrophes, which tend to strike certain geographic areas more than others, and are therefore more predictable). Fears of overwhelming losses from a single event or series of attacks kept many insurers and reinsurers out of the terrorism market after September 11, 2001. A major loss that reverberates nationwide or even globally could have a similarly chilling impact on the cyber market's expansion.

"Bottom line, we really don't know enough about how much exposure we've actually taken on," one insurer told us. "We don't know enough about where the source of the risk is so we can mitigate it. We don't have enough data to help on the underwriting side so they are aware what really makes sense for each segment."

A separate, but perhaps equally troubling, aggregation dynamic seems to be playing out in the small-business market. Here, many carriers are offering to add cyber risk endorsements to standard property and liability policies to attract and retain insureds in a competitive market—sometimes for little to no increase in premiums. This has raised alarm bells among some rating agencies as to whether insurers may be accumulating a substantial, yet underfunded exposure on their books, especially if a systemic event impacts a wide range of insured small businesses all at once.

Tunnel vision is limiting the appeal of cyber insurance products

Another concern is that a relatively narrow view of what constitutes cyber risk may be prompting many insurers to focus their marketing efforts primarily at those facing the possibility of PII theft. However, those we spoke with said such coverage is rapidly becoming commoditized and price-sensitive, limiting long-term insurer growth and profit potential.

More importantly, there are many other, more complex risks arising that might benefit from cyber coverage, beyond PII concerns. Indeed, what good is cyber coverage for PII at a company that doesn't hold sensitive consumer records?

Take the case of a manufacturer running an industrial control system with the help of IoT technologies. What if its operations are compromised by those who either shut it down maliciously and/or sabotage the products it is producing? Then there are the unique risks facing makers of autonomous passenger vehicles, which could theoretically be activated remotely by hackers and then stolen or misdirected into accidents.[9] It is also conceivable that autonomous commercial trucks could be hijacked remotely in a cyberattack. Are these emerging exposures covered by standard liability policies, or might a specific cyber endorsement or stand-alone cyber policy offer a more certain risk-transfer alternative?

These are the kinds of fundamental questions insurers should confront as they consider entering or expanding their presence in the increasingly complex cyber risk market.

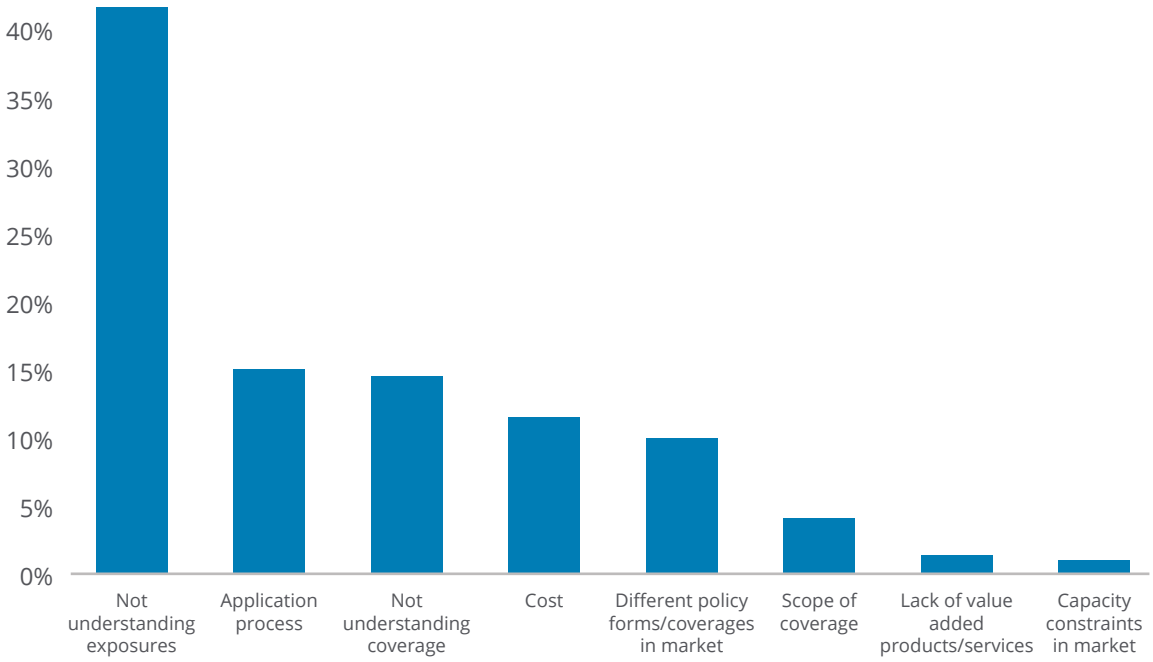
Obstacles from the cyber insurance buyer's perspective

Buyers often don't understand cyber risks or their insurance options

Insurers likely aren't the only ones hampered by a lack of data or reliable predictive models when it comes to contemplating the value and viability of cyber insurance. The brokers we interviewed tell us that buyers large and small also can have a hard time quantifying exactly how big a risk they face. That may lead to uncertainty about what type of coverage and how much insurance they might need, as well as the cost/benefit associated with transferring at least part of this burgeoning exposure to insurers.

Indeed, many consumers—and not just unsophisticated buyers running small businesses—often aren't even aware of the cyber risks confronting them, let alone the insurance coverage options available. A survey by PartnerRe and Advisen found that 42 percent of brokers cited clients "not understanding exposures" as by far the biggest obstacle keeping them from selling more cyber insurance (see figure 3).[10] In addition, 55 percent of brokers surveyed by the CIAB in October 2016 said there isn't enough clarity about what cyber insurance covers.

Figure 3. Brokers cite top obstacles to cyber insurance sales



Source: PartnerRe in collaboration with Advisen, "Cyber liability insurance market trends: Survey," August 2015.

While this shows an improvement over the 71 percent who felt this way in the CIAB survey a year earlier, it still represents a majority of those placing the coverage with bigger buyers.[11]

Value is another concern, as the brokers we interviewed told us that many large commercial buyers wonder whether the coverage being offered by insurers is sufficient for the risks they face or the premiums they're being asked to pay. At present, cyber policies often are capped with relatively low limits for the risks being covered, which brokers told us may be discouraging more buyers from taking the plunge. Only 48 percent of CISOs and other security professionals surveyed by the SANS Institute and Advisen Ltd. said cyber insurance is at least "adequate" when addressing the consequences of a cyber breach.[12]

In addition, for many prospects, coverage for emerging risks may not yet be widely available or affordable. As noted earlier, those dependent upon the IoT to run their operations may face an entirely different set of exposures from those concerned about the loss of PII, yet breaches related to customer data are getting a lot more attention in the media and the insurance marketplace. That narrow approach likely has to be widened if insurers are to realize the bullish growth predictions being issued about the market's future.

Cyber risk can be spread over a wide range of coverages

Part of the problem with selling cyber insurance, according to the brokers we queried, is that cyber risk may be included as part of a wide range of products—including general liability, property, professional liability, business interruption, and crime policies, among other standard coverages. This complicates efforts to assess coverage needs, match policies with exposures, and compare alternatives. It also challenges buyers and their intermediaries to figure out where best to place coverage for cyber-related expenses such as forensics, notification, credit monitoring, public relations, reputational risk, legal defense and settlement costs, crisis management, recovery costs, and regulatory fines.

Meanwhile, as the exposure continues to evolve, new cyber risks are emerging regularly—begging the question of where best to place them. Take the case of the hacking and release of confidential campaign emails during the recent US presidential election. Similar risks may face the private sector, if company executives' confidential emails or internal reports are hacked, leading to the release of damaging material via mainstream news outlets or social media. This could result in a wide array of losses, such as trading on inside information, damage to a company's brand, or undermining its stock price.

Until these issues are sorted through, confusion in the market could hinder the sale of cyber coverage among buyers who can't make heads or tails of what coverage they need vs. what they may already have in existing policies.

Cyber policies lack standardization

A complicating factor is that typically the description of coverage terms, conditions, and exclusions are anything but standardized in cyber policies. A study this year by the SANS Institute and Advisen, Ltd. found that only 19 percent of brokers and 30 percent of underwriters said there is a common language of cyber risk.[13] In addition, many respondents to the CIAB's October 2016 cyber insurance survey reported that coverage is often being written via customized policies, resulting in different terminology from carrier to carrier.[14]

> Many buyers remain leery about purchasing coverage; they are afraid they won't realize what isn't covered until after they file a claim.

Indeed, similar cyber insurance products offered by different providers often include alternative features, which makes it difficult for buyers to compare policies by value and price. One major broker we interviewed told us many believe that the industry has a "serious branding issue on its hands," in that while there are so-called "cyber policies" on the market, it's often not clear to the buyer exactly what such coverages entail, and whether they are comprehensive in terms of the exposures they address.

Given all the potential confusion surrounding which policies may cover which cyber risks, as well as what the differing language among policies may actually mean when an event occurs, brokers we spoke with told us that many buyers remain leery about purchasing coverage; they are afraid they won't realize what isn't covered until after they file a claim.

Indeed, concern over potential gaps in coverage—within a policy or among multiple policies addressing cyber risk—seems to be a major reason why many businesses are passing for now. According to brokers we interviewed, these businesses are awaiting additional clarity and for the market to shake out a bit. They want to avoid buying coverage they don't fully understand and whose language may still be subject to interpretation.

The legal landscape remains in flux

Brokers told us that even under the best of circumstances, if one event could be covered under multiple policies from different carriers, and if policy language isn't entirely clear or at least standardized, such conflicts could prompt settlement disputes that might hinder efficient claims management.

In a worst-case scenario, brokers we interviewed said some buyers fear having to litigate a disputed claim due to differences over which policy applies or whether policy language indicates coverage, which might ultimately leave buyers uninsured for a major loss.

One of the carrier respondents we spoke with observed that "cyber coverage disputes have not made their way through the court system yet. Policy terms and conditions have therefore yet to be battle-tested because case law isn't clear." This carrier also cited the "mish-mosh of redundant and sometimes conflicting state regulations that can create exposures and coverage gaps."

This lingering uncertainty likely makes it that much harder for insurers to quantify the exposure they are taking on when they write a cyber policy, and for buyers to appreciate how much exposure is actually being taken off their hands with the policies currently being sold.

Next steps?

Brokers told us that as a result of the obstacles listed above, many insurers are merely "experimenting" in the cyber market as they gather data and first-hand experience. At the same time, one broker observed that given the uncertain state of this emerging market, many buyers are putting off purchasing cyber coverage until they become better informed about the threats they face, as well as the risk management and insurance options at their disposal.

In our next section, we'll explore what steps might be taken to alleviate such concerns. We'll also look at what could be done to get insurers more engaged in this promising growth market, while convincing more prospects to get a better handle on their exposures—in part by buying cyber coverage.

Strategies to overcome cyber insurance growth obstacles

Data-challenged cyber insurers can buy time with alternative approaches

Most insurers likely have their work cut out for them in seeding the field for a much more bountiful cyber insurance harvest. They'll need to overcome—or at least compensate for—many of the obstacles to growth cited above. Two of their biggest challenges are the relative dearth of cyber risk data, as well as concerns over quantifying and coping with potential loss aggregation.

Those we spoke with conceded that without sufficient historical data and with a constantly evolving threat to assess, pricing for cyber coverage is likely to remain something of a work in progress for quite some time, making trial and error the de facto operating strategy for most carriers. Many insurers may simply have to write more cyber business over the next few years to gain the critical mass of data and experience needed to break the "vicious circle" hampering more rapid growth. While potentially slowing down the pace of expansion in the short term, cyber insurance underwriters will likely have to learn to walk before they start running full speed ahead into this rapidly developing, and still uncertain, market.

In the meantime, insurers may want to adjust expectations and avoid trying to create a definitive predictive model that could be quickly rendered obsolete in a shifting threat landscape. Instead, they could focus on producing a "risk-informed model" in which underwriting and pricing assessments would emphasize specific risk-management steps applicants could take to be secure (prevention), vigilant (detection), and resilient (loss control and recovery) in their cyber-related operations.

With this approach, many insurers could perhaps leverage their internal cybersecurity expertise to facilitate external business growth. In defending themselves from cyberattacks, insurers often have threat intelligence units to collect and analyze data for their own risk-management needs. Such resources could perhaps be externalized to inform smarter underwriting and pricing of cyber coverage.

The insurers we interviewed didn't draw upon their own company's firsthand cybersecurity experience to help them assess the maturity of prospective clients' loss-control programs, and the brokers we spoke with said that was the case across most of the industry. Such silos should perhaps be taken down to benefit not just the underwriting department, but internal risk management as well. This could help insurers learn something new from the experiences and approaches of their diverse group of policyholders, similar to the benefits of shared loss-control experience in workers' compensation and property-catastrophe exposures.

Insurers might also offset their data disadvantage somewhat by adopting a segmentation approach to underwriting. This would narrow the scope of cyber expertise required of underwriters by targeting specific industries or niches within them. Alternatively, insurers could become specialists in a certain type of exposure (such as data breaches vs. denial of service attacks) or area of technology (such as the IoT or domain name servers), rather than write generic cyber policies across the risk spectrum, so as to have a better handle on the exposures being assessed.

To ease concerns about the potential for a catastrophic aggregation of loss, particularly in the large-account segment, brokers suggested that insurers might consider taking a slice of a layered, multi-insurer coverage program. This option would

limit a carrier's individual exposure while providing adequate overall protection for the insured.

In addition, heavier reinsurance involvement could help ease the primary market's aggregation burden and encourage more aggressive growth. Brokers we spoke with indicated that reinsurers seem poised to become more involved in covering cyber exposures, a finding echoed by recent media reports. *Best's Insurance News* reported that "as traditional property-casualty reinsurance markets remain soft, reinsurers are increasingly looking to niche markets for new revenue streams, and one of the hottest is cyber coverage." However, the article added, "The challenge is to gain profitable market share in a line the carrier may not know enough about."[15]

Insurers could offer holistic cyber risk management programs

Longer term, it may be time to redesign the cyber insurance product altogether, differentiating policies beyond their price, terms, and coverage limits to emphasize associated risk-management service offerings. This would entail creating comprehensive, holistic programs that span a buyer's cyber risk life cycle to complement traditional risk-transfer provisions.

> Insurers should consider implementing a more rigorous process to underwrite and price cyber policies based on a buyer's risk-management maturity.

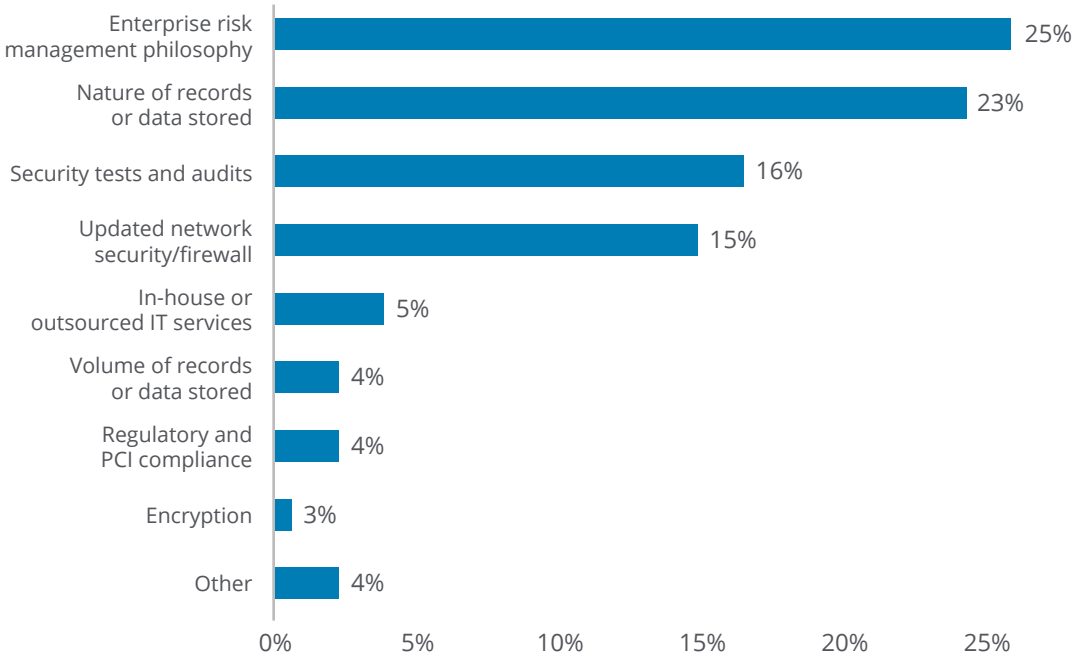
Risk prevention services, as well as post-loss response and recovery support, might be offered to secure the client's cyber insurance purchase, while helping bolster retention of the account and making relationships with clients more dynamic. The latter goal could be accomplished via real-time monitoring, while offering lower premiums and/or increased limits as reward incentives for policyholders that meet or surpass risk-management maturity benchmarks.

Becoming a client's full-service cyber risk manager as well as their chief risk-transfer vehicle could be advantageous for both buyers (by helping prevent incidents from happening in the first place) and insurers (by lowering loss frequency and severity, while increasing the likelihood of retention). Here again, an insurer's internal risk-management team might be useful in business development by sharing their hard-earned insights and expertise with clients facing similar types of exposures. Taking this a step further, cyber insurers could differentiate and add value by externalizing their own threat intelligence capabilities to provide alerts and risk-management suggestions for insureds.

Since the industry appears to need time to gather and analyze more data, and given the inherent unpredictability and volatility of this evolving risk, insurers should consider implementing a more rigorous process to underwrite and price cyber policies based on a buyer's risk-management maturity. Many insurers already seem to be heading in this direction, in terms of the value they are placing on a prospect's enterprise risk-management philosophy when it comes to assessing cyber risk (see figure 4).[16]

In the absence of data, it likely makes sense for insurers to scrutinize cyber coverage applicants more rigorously. While perhaps not practical with smaller insureds, whose coverage needs and risk-management maturity might be adequately assessed via questionnaires, larger organizations seeking standalone coverage should perhaps be handled the same way major commercial property insurance applicants are qualified. This process often involves an on-site inspection and even ongoing monitoring of their loss-control capabilities. Brokers told us that's not generally the case today with cyber applicants, which makes many insurers hesitant to write the broader coverage or higher limits that could generate more sales among bigger prospects.

Figure 4. What do underwriters value in assessing a cyber risk?



Source: Hanover Research/Market Insight Center, "Cyber liability insurance market trends: Survey," prepared for ISO, November 2014.

Overall, adopting a risk-management-based approach could give insurers some breathing room to collect more data and bolster their predictive models for the long haul. It could also improve their immediate competitive position and enable them to expand cyber writings more aggressively in the interim.

Insurers, intermediaries should keep raising risk awareness

Most large companies likely have a basic awareness that they may face serious cyber exposures, thanks to the growing number of cyber-related events reported in the media impacting businesses, foundations, governments, political parties, and individuals. Indeed, last year's PartnerRe survey of underwriters and brokers found that the top driver of cyber sales by far (cited by nearly two-thirds of those queried) was "news of cyber-related losses/experience by others" (see figure 5).[17] Such publicity often prompts greater attention to cyber risks by the boards of public companies. In our earlier report on cyber risk management at financial institutions, CISOs told us that such board interest puts pressure on a company's management team to demonstrate that they have high-profile cyber exposures contained and covered.[18]

One carrier we interviewed told us that as the "fear factor" expands—that is, as more prospective buyers read about events in the media, hear about them from business colleagues, see them striking competitors, or experience them firsthand—appreciation of the risk (and, hopefully, the corresponding demand for cyber coverage) should rise and accelerate over time.

However, insurers shouldn't merely wait around for media coverage to keep current and prospective policyholders informed about the risks they face and how to cope with them. Instead, the industry should be more proactive in creating better-educated consumers and thereby encourage more businesses to implement risk-management programs and buy coverage. One way to accomplish this is by enhancing direct outreach efforts via marketing and advertising. Another, more personal approach is to

deploy their intermediaries to explain and promote the coverage.

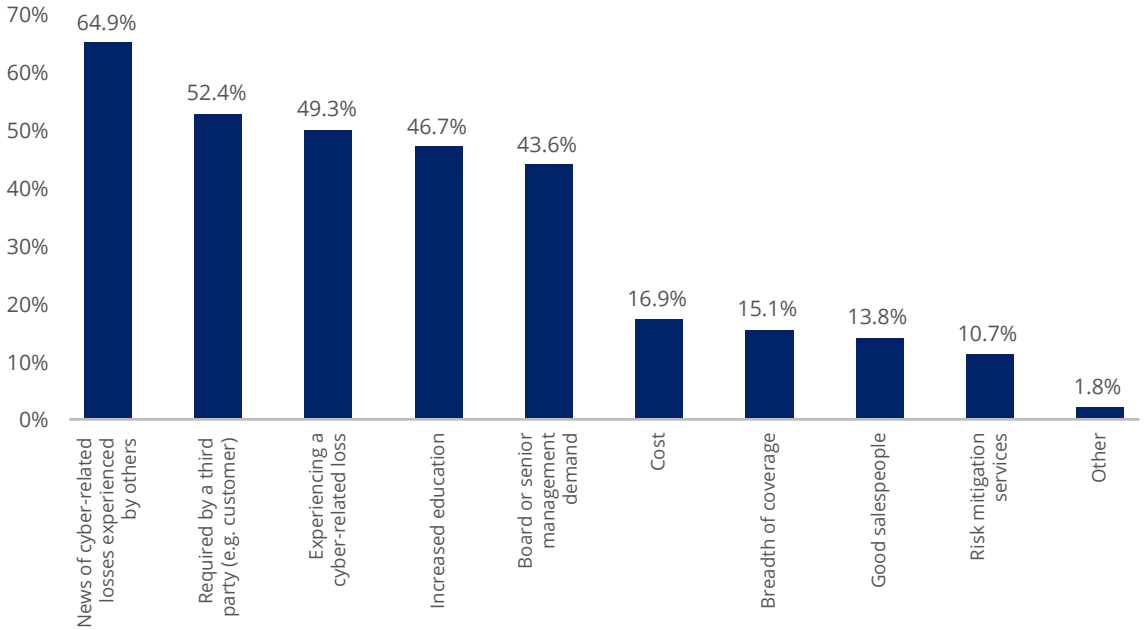
The vast majority of larger brokers already appear keen on providing such information to policyholders. Indeed, the latest CIAB survey found that 88 percent of respondents have "some sort of proactive, strategic approach to educating clients and prospects about cyber risk."[19] Yet the effectiveness of such efforts has been rather limited, as only 37 percent of those surveyed said their clients have in place a "proactive information security program." This, according to the CIAB, "suggests that progress is slow as entities struggle to stretch tight budgets to adopt cyber defenses."[20]

In addition, while global and regional brokerages may have the resources and expertise to take on this educational assignment, smaller independent agencies could have a problem keeping up. Such agents tend to deal with small business accounts that generate relatively low premium and commission payments, therefore providing little incentive for them to do more than pitch add-on cyber endorsements to standard policies.

Cyber insurers can help support small and big intermediaries alike by providing risk awareness and loss control materials. These may include tip sheets, websites, and podcasts, as well as referrals to cybersecurity specialists (including perhaps the insurer's own risk-management services division, or cybersecurity firms partnering with the carrier).

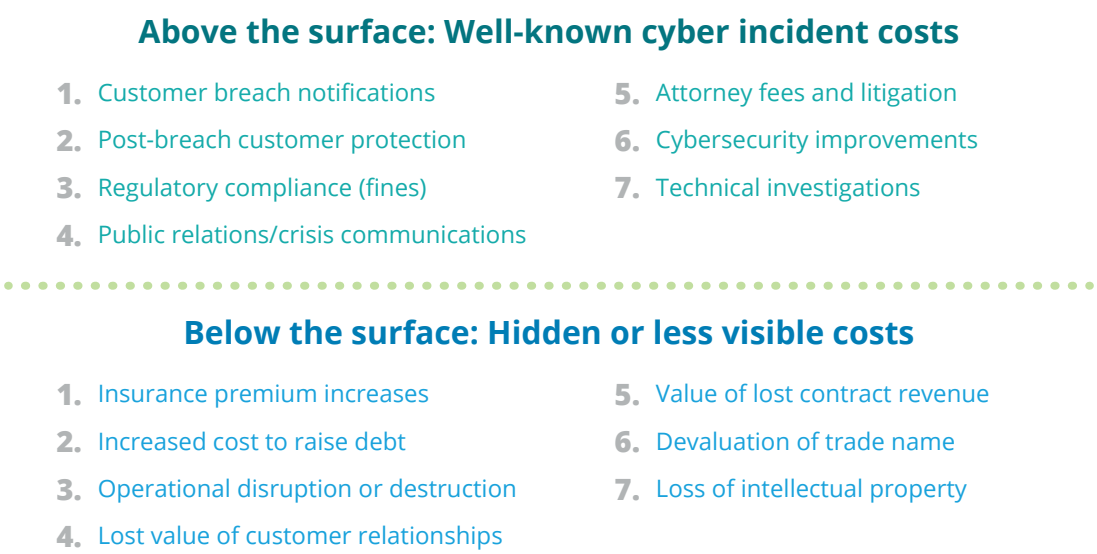
One carrot to possibly convince agents to get more heavily into cyber education is the potential to generate additional fee income from risk-management services. Another may be to avoid disintermediation by evolving from being price-driven policy peddlers into more value-added risk managers, at least for their larger commercial accounts. A third incentive might be to avoid costly errors and omissions claims if they neglect to advise clients to buy cyber insurance, or fail to explain to them that certain cyber risks are not included in their current coverage. Finally, agents and brokers could be reminded about their own cyber exposures, given the treasure trove of data they collect from clients, and could be prompted to share that experience and expertise with customers—including the purchase of cyber coverage for their agencies.

Figure 5. Top drivers of cyber sales



Source: PartnerRe in collaboration with Advisen, "Cyber liability insurance market trends: Survey," October 2016.

Figure 6. Costs of a data breach



Source: "Beneath the surface of a cyber attack: A deeper look at business impacts," Deloitte Cyber Risk Services.

A big part of the education process is to inform clients about the potential costs of a cyber event, both above and below the surface. Take data breaches, for example (see figure 6). There are well-known cyber incident costs to account for, such as customer breach notifications, but also less obvious expenses such as the value of lost contract revenue or the loss of intellectual property. This can lay the groundwork for a more informed sales presentation and purchase decision.

Standardizing policy language could boost consumer confidence

To resolve confusion over which policies cover what, brokers and insurers alike told us that greater standardization of verbiage in forms is likely necessary. "There needs to be standardization so that we know what we're selling and the client understands what they are buying," noted one respondent to the most recent cyber survey by the CIAB, which observed that "many brokers feel that a common lexicon would be tremendous in helping clarify cyber policy language."[21]

ISO noted that standardization in terminology could help avoid "massive" potential for coverage disputes along with the lengthy and costly litigation that might result. However, as an additional benefit, ISO observed that "standardized policy form wording also serves as a launch pad by which companies can innovate their proprietary products and solution offerings—helping to accelerate their entry into the marketplace with more confidence, speed, and efficiency."[22]

Standardization won't necessarily come easily. It will likely require collaboration and cooperation among industry competitors, as well as with neutral third parties such as trade associations and standard-setting organizations.

In the long run, standardization should lower the chances for potential coverage disputes that raise claims management costs for insurers, undermine consumer confidence in the certainty of their coverage, and hinder efforts to increase sales. Ultimately, establishing standards in cyber policies could enable those already selling products to write more business, while easing entry for additional players.

Where do cyber insurers go from here?

CONSIDERING the maturity of their long-established markets, organic growth can be hard to come by for property and casualty insurers, even in the best of times. But achieving sustainable growth seems even more problematic than usual these days given the overcapacity in many primary and reinsurance sectors. For the short term, stiff competition is generally keeping prices down, limiting gains in premium volume and undermining bottom-line profitability. Looking further down the road, the looming specter of driverless vehicles and ridesharing may prompt a downsizing of epic proportions in the industry's biggest line of business, auto insurance. Disruption of the labor force through automation could create turbulence for the industry's largest commercial line, workers' compensation. In the midst of such challenging conditions, cyber insurance appears to offer one of the few opportunities for substantial, long-term growth.

The industry's initial experience has been positive, with the loss and loss adjustment expense ratio for cyber coverage coming in at 42 percent for 2015—although that figure was much higher for stand-alone policies (51 percent) than for coverage included in package policies generally written for smaller businesses (only 34 percent).[23] This experience compares quite favorably with the five-year average for many standard lines, such as workers' compensation (77.4 percent), commercial auto (75.9 percent), and commercial multi-peril (66.8 percent).[24]

However, conditions could change in a hurry—one way or another. Some we spoke with expressed concern about the potential impact of a sudden increase in the severity of losses, particularly a systemic cyber event that triggers a wide range of claims across industries. One broker observed that "underwriters didn't really charge for terrorism exposure. Then 9/11 hit. Underwriters will worry, 'Do we have a 9/11-level event coming in cyber?'" The broker noted that the 9/11 attacks prompted the market for terrorism coverage to virtually dry up overnight—a condition that persisted until a federal reinsurance backstop was put in place to entice insurers to return and offer more affordable coverage. (Indeed, a number of those we interviewed wondered whether a massive cyberattack could be classified as terrorism under certain circumstances, and whether specific cyber-terrorism endorsements might be required, thus introducing another layer of uncertainty into the cyber coverage debate.)

On the other hand, some we interviewed expressed concern about too many players rushing in to write cyber coverage as part of a new "gold rush," flooding the market with what one broker referred to as "naïve capacity" and pressuring insurers to cut rates and expand coverage to attract and retain business. It's almost like the story of Goldilocks—will the cyber market heat up too quickly, will a huge event cool it off suddenly, or will conditions remain just right to foster a stable, steadily growing segment? The answer will be largely determined by how insurers set up shop and handle this volatile risk.

It's also important for traditional carriers to keep in mind that an insurance policy isn't the only

Cyber insurance appears to offer one of the few opportunities for substantial, long-term growth.

risk-transfer option for buyers when it comes to covering cyber risks. Bigger buyers are likely to consider alternatives they have tapped in the past when insurance coverage became scarce or too expensive—such as captives, risk retention groups, and securitization. Consider how the property-catastrophe market has been disrupted by cat bonds and other insurance-linked securities—particularly the impact on the reinsurance sector. Prices and profitability in the traditional insurance market have plummeted as a result.[25]

Might cyber bonds be floated one day soon to help large organizations transfer their exposure to investors in the capital markets, rather than via traditional insurers? Along the same vein, will cyber risk retention groups be formed to cover groups of small to midsize companies? Or might cyber captives be launched on- and off-shore to facilitate self-insurance and offer buyers direct access to the reinsurance market?

These are all very real, even likely possibilities, especially if insurance coverage continues to be perceived by many buyers as insufficient, uncertain, overly complicated, and/or too costly for the value offered.

To avoid displacement by alternative markets as well as by more proactive traditional competitors, carriers should be actively weighing options to facilitate their entry or expansion in this promising but problematic market—including whether they may need outside help. Among the fundamental questions insurers should keep in mind as they formulate their strategies:

- Can we assess this risk with our current resources? Or should we purchase external data or third-party models to support underwriting and pricing systems, at least for the short term?
- How might we work within the industry to standardize our policy language, while still leaving room to differentiate via additional coverage and service options?
- What can we learn from our own direct experience as insurance organizations managing cyber risks? How might we leverage that expertise to support our underwriting, pricing, and risk management services for clients?

The latter point might be the most important in both the long term and short term. As a high-profile target of hackers, the insurance industry knows cyber risk firsthand. They are grappling with many of the same exposures and risk-management challenges as those seeking coverage from them. While their levels of risk-management maturity might differ, they generally appreciate how unpredictable the risk can be, how difficult it is to detect, prevent, and contain, as well as how much damage an event could cause. So it shouldn't be a surprise that many insurers have been cautious about expanding their cyber business or even entering the market in the first place.

But being in the business of risk, the industry is also in a prime position to capitalize on what is likely to be increasing interest in the purchase of cyber insurance—that is, if they can crack the code before buyers find another way to cover their exposures.

ENDNOTES

1. Robert P. Hartwig and Steven N. Weisbart, "2015 year end results," Insurance Information Institute, May 16, 2016, http://www.iii.org/article/2015-year-end-results.
2. Robert P. Hartwig and Claire Wilkinson, "Cyber risk: Threat and opportunity," Insurance Information Institute, October 21, 2015, http://www.iii.org/white-paper/cyber-risks-threat-and-opportunities-100715.
3. Carrier Management, "Cyber risks poised to become a $20 billion dollar market," Wells Media Group, September, 2015, http://www.carriermanagement.com/news/2015/09/13/145178.htm.

4. The Council of Insurance Agents and Brokers (CIAB), "Cyber insurance market watch survey," October 26, 2016, https://www.ciab.com/uploadedFiles/Resources/Cyber_Survey/102016CyberSurvey_Final.pdf.

5. CIAB Cyber Market Watch, "Cyber insurance market watch survey," The Council of Insurance Agents and Brokers, September 2015.

6. Celine French and Lisa Hamilton, "Consumer data under attack: The growing threat of cybercrime," Deloitte Consumer Review, The Centre for Economics and Business Research, Deloitte LLP, 2015, https://www2.deloitte.com/tr/en/pages/risk/articles/consumer-data-under-attack.html.

7. Robert P. Hartwig and Claire Wilkinson, "Cyber risks: The growing threat," Insurance Information Institute, June 2014, http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf.

8. Sam Friedman, "*Taking cyber risk management to the next level: Lessons learned from the front lines at financial institutions,*" Deloitte University Press, June 22, 2016, https://dupress.deloitte.com/dup-us-en/topics/cyber-risk/cyber-risk-management-financial-services-industry.html.

9. Alexa Liautaud, "Autonomous car era brings risks of hijacking by hackers," *Automotive News*, September 4, 2014.

10. ParnerRe and Advisen, "Cyber liability insurance market trends: Survey," October 2015, http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2015.pdf.

11. CIAB, "Cyber insurance market watch survey, 2015."

12. Barbara Filkins, "Bridging the insurance/infosec gap: The SANS 2016 cyber insurance study," SANS Institute and Advisen Ltd., June 2016, http://www.advisenltd.com/2016/06/21/bridging-the-insuranceinfosec-gap-the-sans-2016-cyber-insurance-survey/.

13. Ibid.

14. CIAB, "Cyber insurance market watch survey, 2016."

15. David Pilla, "Reinsurers look to cyber as key niche expansion market," *Best's Insurance News*, November 23, 2016, ©AM Best, used with permission.

16. ISO and Hanover Research/Market Insight Center ,"Cyber insurance survey," November 2014, http://www.verisk.com/downloads/emerging-issues/cyber-survey.pdf.

17. "2016 Survey of Cyber Insurance Market Trends," PartnerRe in collaboration with Advisen survey, October 2016.

18. Friedman, "*Taking cyber risk management to the next level*."

19. CIAB, "Cyber insurance market watch survey, 2016."

20. Ibid.

21. Ibid.

22. Maroun Mourad and ISO, "How carriers can unlock the multi-billion dollar cyber marketplace," PropertyCasualty360.com, August 11, 2016.

23. Data from S&P Global Market Intelligence.

24. Ibid.

25. Andrew Mais, "*Securing tomorrow: The ripple effect of insurance-linked securities in the reinsurance market*," Deloitte Center for Financial Services, Deloitte Development LLC, January 2016, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-securing-tomorrow-insurance.pdf.

ABOUT THE AUTHORS

SAM FRIEDMAN

Sam Friedman, senior manager, Deloitte Services LP, is the insurance research leader at the Deloitte Center for Financial Services, where he analyzes the latest trends and identifies the major challenges confronting the property-casualty and life insurance industries. Friedman joined Deloitte in October 2010 after 29 years at *National Underwriter P&C*, where he served as editor-in-chief. Follow Friedman on Twitter at @SamOnInsurance, as well as on LinkedIn.

ADAM THOMAS

Adam Thomas is a principal in Deloitte's Cyber Risk Services practice. He has more than 15 years of experience in the field of information systems. Over the past seven years, Thomas has focused on helping design and implement information technology risk management and information security programs for Deloitte's most significant, complex, regulated global financial services clients. He provides counsel to senior leaders and the boards of some of Deloitte's largest banking and insurance clients on various cybersecurity-related matters.

Prior to his current role, Thomas was in Deloitte's technology risk management center of excellence, where he was responsible for building out the firm's information security and technology risk advisory client-delivery capabilities.

ACKNOWLEDGEMENTS

The Center wishes to thank the following Deloitte professionals for their support and contributions in researching and writing this report:

John Lucker, advisory principal, Deloitte & Touche LLP

Michelle Canaan, manager, Deloitte Center for Financial Services, Deloitte Services LP

Nikhil Gokhale, manager, Deloitte Center for Financial Services, Deloitte Support Services India Pvt. Ltd.

The Center wishes to thank the following Deloitte professionals for their support and contributions in editing, designing, producing, and distributing this report:

Lisa DeGreif Lauterbach, financial services industry marketing leader, Deloitte Services LP

Michelle Chodosh, marketing manager, Deloitte Center for Financial Services, Deloitte Services LP

Courtney Scanlin, senior marketing manager, Deloitte Services LP

Junko Kaji, senior manager, US Eminence, Deloitte Services LP

Karen Edelman, manager, US Eminence, Deloitte Services LP

Kevin Weier, art director, Deloitte University Press, Deloitte Services LP

Chris Lyons, illustrator

CONTACTS

Industry leadership

Gary Shaw
Vice chairman
US Insurance Leader
Deloitte LLP
+1 973 602 6659
gashaw@deloitte.com

Deloitte Center for Financial Services

Jim Eckenrode
Executive director
Deloitte Center for Financial Services
Deloitte Services LP
+1 617 585 4877
jeckenrode@deloitte.com

Authors

Sam Friedman
Insurance research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Adam Thomas
Advisory principal
Deloitte & Touche LLP
+1 602 234 5172
adathomas@deloitte.com

 Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

About Deloitte