Insurance 2025

Reducing risk in an uncertain future

IBM Institute for Business Value

How IBM can help

Maturing markets, tight capital, increasing risk and technologically sophisticated customers are just some of the pressures the insurance industry faces today. As a result, insurers will have to work faster, more efficiently and, above all, smarter. Those that do will thrive; those that don't will fail. Insurers need to be more nimble, innovative and connected with their customers. The IBM Global Insurance team has reinvented itself to provide solutions to help clients meet the demands of today's insurance business. From enhanced customer service to greater efficiency in the back office and improved risk management, there's a smarter solution for you. For more information about IBM Insurance solutions, visit **ibm.com**/insurance.

Prevention-as-a-service, wherever you are

Expansion of capabilities in cognition and "edge computing" have reached critical mass and the repercussions will be long-lasting, but the impact on insurance business models is far from certain. Scenario consideration reveals some no-regret plays for insurers that should secure a seat at the table no matter the outcome — and no matter which tables end up ultimately handling the business of risk management.

Executive summary

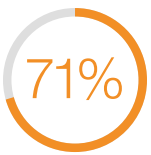
Ever since Greeks consulted the Oracle of Delphi before undertaking a war or business venture, fortune tellers and soothsayers have done a brisk business. Whether in our personal lives or in our business dealings, we would like to know what will happen so we can be prepared. These days, predictions have shifted from magical to scientific, yet, as the old Danish proverb goes, "Prediction is very difficult, especially about the future."[1] In this executive report, we attempt to look into the crystal ball anyway — to help insurers prepare for the future.

This report is based on a series of insurance and CxO studies conducted by the IBM Institute for Business Value over the past few years, in combination with a number of informal conversations and discussions with subject matter experts and insurance executives.

We look at two key technology waves — cognitive computing and systems decentralization — that will have significant impact on the future of business across industries and that will affect insurance companies and their customers. However, considerable uncertainty surrounds their adoption pattern, and so we will consider scenario planning regarding the various potential outcomes of these two waves:

1. How will cognitive technologies be deployed — as utilities or as proprietary tools?
2. Will operations and decision-making happen on "the edge" in distributed models, or centrally in common processes?

79 percent of insurance CxOs say they believe **technology will have a major impact** on their organizations



71 percent of insurers indicate they **have begun using cognitive** technologies

By **2050**, more than **100 billion connected devices** are expected to be in use

The answers to these questions will impact value chains across industries and influence how individuals and organizations interact, how they view risk and what their future insurance needs will require:

- In "*the swarm economy*," self-organizing and intelligent distributed systems strongly compartmentalize and localize risk
- In "*central intelligence*," risk prediction becomes highly specialized as expert systems augment humans to optimize sales, service and claims decisions
- In "*the Internet of Everything*," instrumented systems place high emphasis on risk measurement, management and feedback
- Finally, in "*survival of the fastest*," cognition and edge data become an arms race, with deep investment competitors building insurmountable leads.

We will then discuss logical next steps for insurers to navigate cognition and distributed computing, along with some "no-regret" moves that will help insurers prepare for the future, regardless of outcomes.

Four possible futures

For a number of years, we have tracked the main forces that concern C-suite executives. The priorities for insurance leaders today are quite clear, with the top three factors being, by a large margin, regulation, market forces and technology.[2]

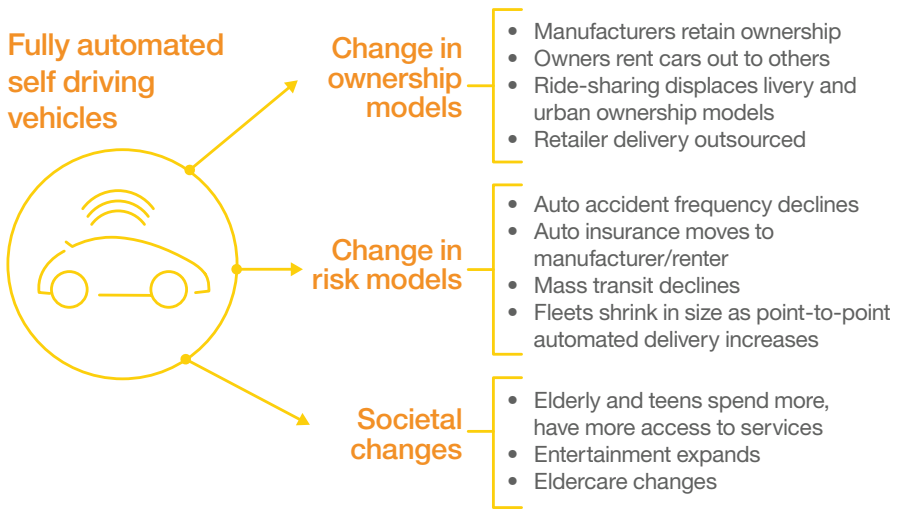
Technology, especially, used to be perceived by insurers as a means to an end, a tool to cope with changes in markets and changes in regulation. But insurers have increasingly made technology integral to their products and business models. Technology has become both a threat to enable new industry entrants, as well as an opportunity to extend insurance across traditional industry boundaries.

As an example, consider the potential impacts of an in-progress technology shift: the move to autonomous or semi-autonomous driving. Once autonomous driving becomes more commonplace — and examples are projected to hit the market in 2020 – it will have significant ripple effects on a number of industries (See Figure 1). This will affect insurance both directly and indirectly.

The rise of technology concerns means CxOs must look into the future to build competitive advantage. What good does responding to a hard market do when the industry restructures under your feet? CxOs, now more than ever, need to future-proof their businesses. To do that, they need a longer view. How will the world look in 2025, and what does that imply for the insurance industry?

In our opinion, two technological trends, in particular, will have a high impact on the future of business across industries: the rise of cognitive computing, and the increasing potential for decentralization of systems and decision-making.

Figure 1
Self-driving cars will have ripple effects on many industries



Source: IBM Institute for Business Value

In a *decentralized* system, lower-level components operate on local information to accomplish global goals without a central organizing influence. Devices will be equipped with sensors and actuators, giving them the potential for complete autonomy. Security of transactions can be established via electronic ledger technologies, such as blockchain. The devices needed to establish such a decentralized system are already on the rise and expected to grow exponentially — from 2.5 billion in 2009 to 25 billion in 2020, with more than 100 billion expected in 2050.[3]

Cognitive computing refers to next-generation information systems designed to accelerate, enhance and leverage human expertise. These systems can learn at scale, reason with purpose, and interact with humans naturally. Their ability to handle unstructured data and range across wide subject domains gives them opportunity to remake business processes, and we believe these technologies will have reached maturity by 2025. According to a 2016 IBM Institute for Business Value survey, 90 percent of outperforming insurers say they expect cognitive technologies to have a strong impact on their revenue models, and 71 percent say they have already started using these technologies.[4]

When describing the world of 2025, we see the spread of these two technologies as "forks in the road." Their potential impact is high, but the exact nature of their implementation is uncertain.

For decentralization, the question will be where the center of control will sit, and how fragmented the networks will be. For example, limitations imposed by privacy concerns, regulation, or liability could hamper strong device autonomy and drive centralization of control.

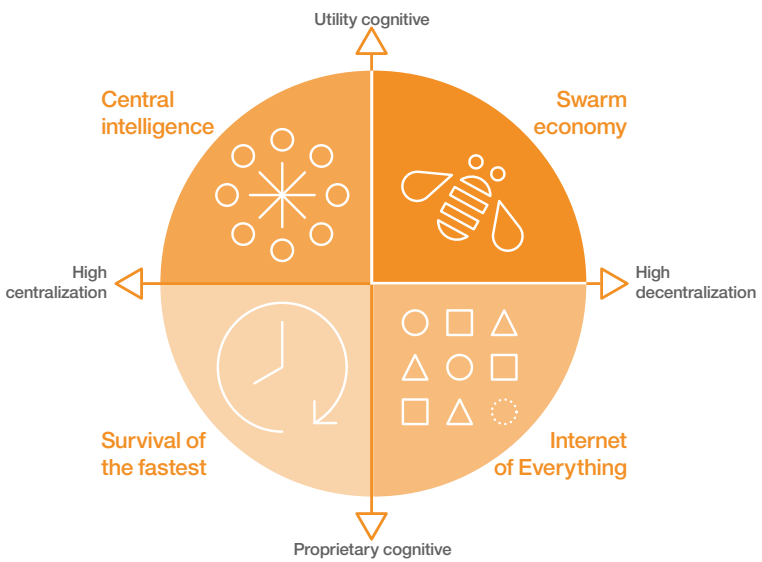
For cognitive systems, variance will be around the depth and ubiquity of adoption: will cognition progress to automated ingestion of rules and decision-making, and will that be deployed as proprietary tools or "must-have" industry utilities?

Using these two technological trends and their adoption variance, we arrive at four distinctive future scenarios. We call these scenarios "central intelligence," "the swarm economy," "the Internet of Everything" and "survival of the fastest" (see Figure 2).

Note that these scenarios describe all industries, not just insurance. They do, however, have implications for risk in general, and for insurance in particular, which we will describe in the following sections.

Figure 2

Different levels of decentralization and cognitive use will shape different futures



Source: IBM Institute for Business Value

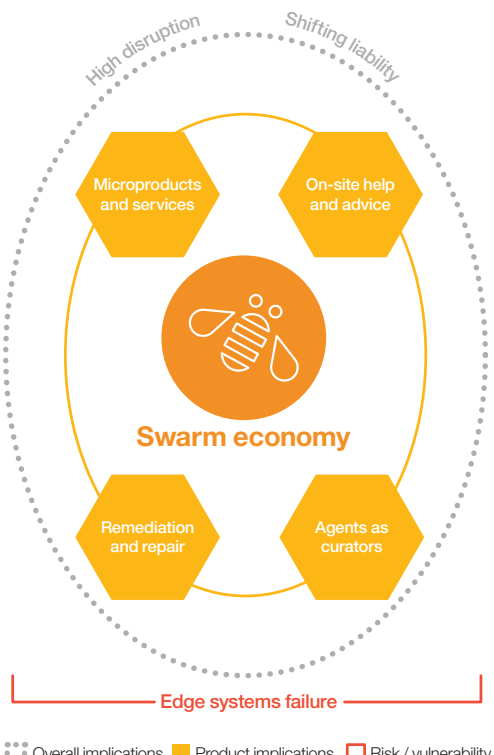
The swarm economy

The swarm economy scenario posits a high adoption rate of both distributed and cognitive technologies. Its name was inspired by the term “swarm intelligence,” an expression introduced in the context of cellular robotic systems, defining the collective behavior of many independent, decentralized, self-organized systems.[5]

In contrast to swarm intelligence, which assumed intelligence emerging from collective behavior of groups of dumb devices, devices in the swarm economy utilize cognitive technology and edge computing to enable distributed decision-making. Each device decides independently of all others how to behave, just as with human actors. Unlike humans, though, these devices connect and communicate with each other, sharing information via standard interchange rules, so that decisions take common and individual factors into account. As an example, an automated home would know what was in the refrigerator, when the owners were likely to be home and when they tend to eat. It could then order missing cooking ingredients, have them delivered and prepare the food as far as possible via automation (for example, through a household robot). In a larger context, devices within an apartment complex could work together, coordinating orders and deliveries, thus increasing efficiency.

The key advantage here is the overall resilience of such systems. While many distributed agents mean many points of failure, cognitive capabilities allow quick response when failure events are noticed. At the same time, automated decision-making at the endpoints introduces new vulnerabilities. Cognitive systems need to surpass human expert reliability over a wide range of use cases. And distributed interactions can lead to emergent system effects if not managed well — a chain of cars using automated following could collectively crash if fog or ice were encountered.

Figure 3
Insurance implications of the swarm economy.



Source: IBM Institute for Business Value

For insurers, the swarm economy would have a highly disruptive impact on classical business and distribution models. Insurance products may move from blanket coverage to micro-services bundled with swarm devices, with an emphasis on local and immediate repair and remediation of losses. Pure insurance would shift to incremental on-site helpers that support and augment human skill, such as for driving or construction safety or nutrition. Distribution of insurance would be much more embedded in day-to-day life, with agents and touchpoint workers becoming relationship managers, curators and broad risk advisors. Automation of decision-making means that liability would shift from individuals to manufacturers or service providers, thus fundamentally changing customer relationships.

Risks for insurers in this scenario would largely be the result of equipment malfunctions or malicious actions: local systems failure, deceit of local sensors (such as odometer hacking) or systems interference. Insurers may not have access to all the data in swarm systems, making risk prediction and management challenging (see Figure 3).

Central intelligence

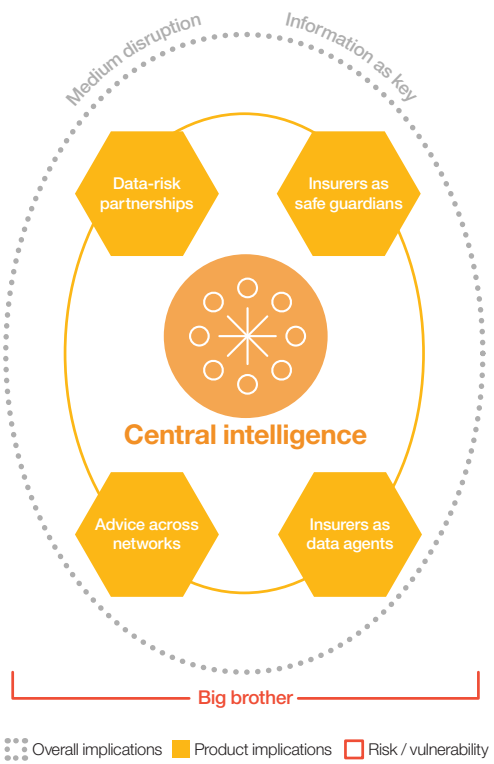
In our second scenario, central intelligence, we assume that most organizations have adopted cognitive technologies as utilities, but that decentralized systems remain limited in capability. System complexity may remain centralized for security reasons, out of privacy issues regarding data sharing, or through difficulties in integrating necessary sensors into accessible ecosystems.

Control and decision-making remain centralized in this scenario. Systems become “eyes in the sky” that pull data in centrally and provide complex judgments, advice and decisions. In our home automation example, each home device has limited ecosystem communication capabilities. Owners would instead manage homes with smart virtual agents and hubs, via cloud-based management of a home automation hub, for example. These centralized agents, a blend of automated support and human direction, would assist human decision-making in what to order, cook or repair. There may be broad coordination among community peers, at the building level, for example.

The key advantage of this future is the ability for deep decision-making — the centralized cognitive systems pair a vast amount of expertise with collected data from unaware edge systems. Its vulnerability lies in communications failure — not an issue as long as (human) expertise is still available at the edge, but problematic when it is not, which is likely as local expertise becomes redundant.

In the central intelligence scenario, information access would be the premier driver of business success for insurers. If partnerships are not available or data communications fail or are hacked, informed decision-making fails too. Insurers with inadequate access to local data networks risk being left behind.

Figure 4
Insurance implications of central intelligence



Source: IBM Institute for Business Value

On the product side, insurers could manage or interface with data hubs to act as agents on customers' behalf. They could negotiate with other (non-insurance) providers to enable bulk buying, discounted access and joint products. And they could manage both individual device and systemic risks through knowledge of the data and interactions being collected. Insurance becomes a "guardian angel" based on day-to-day observation.

Cognitive insights enable insurers to bring value to data-risk partnerships, accelerating a zaibatsu-style combination of insurance with constellations of property, financial and health partner providers. Insurers could also offer advisory and incentive plans across provider networks, such as a discounted life policy for those who exercise, and free smoothies for every ten gym visits. The ability to offer advice customers will take, through psychographic and next-best-action analysis, becomes critical for risk management. Branding would shift to customer identification of safe guardian figures.

Cognitive and artificial intelligence (AI) can empower insurers to assess risk to a high degree on an individual basis, potentially leading to segments of one. This carries the risk of significant regulatory compliance issues, as many customers would see adverse ratings, further decreasing the already low trust consumers have in the insurance industry. Fears of "big brother" would remain a brand risk, as would a tendency for customers to eventually blame insurers for not preventing every peril (see Figure 4).

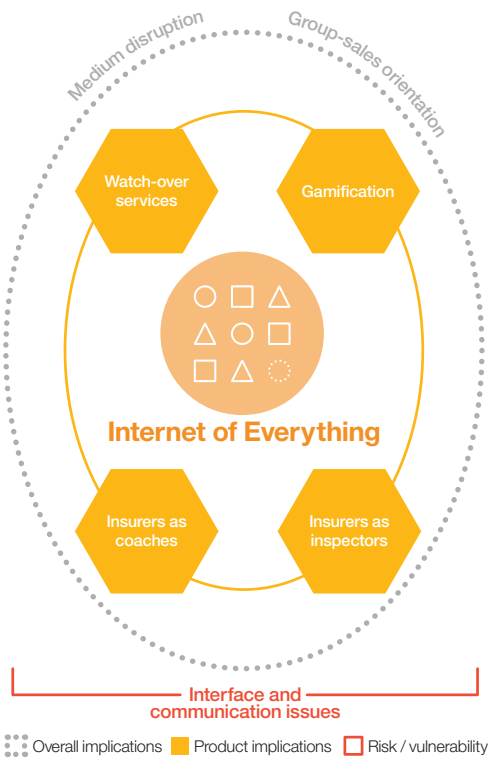
Internet of Everything

A low adoption of cognitive technologies combined with high decentralization would lead to the Internet of Everything scenario. Instead of the smart distributed agents we see in the swarm economy, the instrumented systems in this world would simply be collecting and sharing data. Local AI and non-human advice and decision-making might exist in some cases, but would not be the norm. Again using the home example, the home would be equipped with a multitude of individual sensors and connected devices, providing the owner and/or service providers information about various variables and possible occupant behaviors, from refrigerator contents, to room temperatures, to occupancy. Data may be shared, but it would be shared between devices or between local hubs, with little public access. The human owner would be in charge of the "instrumented home," and decision-making would be entirely human driven, based on local analytics derived from connected sensory data.

The key advantage of this scenario would be to enable a highly individualized "market of one," due to a wealth of information about the individual. The flip side — the scenario's key vulnerability — is the issue of privacy. Public backlash leading to stringent regulation could collapse this scenario to our final one, "survival of the fastest."

In the Internet of Everything, insurance would become more group-sales oriented, potentially via the providers and distributors of interconnected devices, as these relationships would trump most other differentiators. Current experience with this model suggests a high emphasis on local support. Human interactions are frequent and significant in building brand, and so interactive experience design and process design would become paramount, since users quickly grow frustrated and disengage from systems they cannot understand.

Figure 5
Insurance implications of Internet of Everything



Source: IBM Institute for Business Value

In an environment in which data access is decentralized, those who have access gain a significant edge in product deployment and insured interaction frequency. In consequence, insurers would need to measure and track the net value of the information used. Negotiated access to data would be a precondition for the provision of risk services; with enough customers willing to share, there would be a shift among insurance products to "the quick and the dead" —products that bundle data access would earn better rates and more profitable risks; those that do not would be undesirable and rated accordingly. Insurers will need to manage regulatory and discriminatory practice issues, but the differential between data-linked and "blind" risk would become too great to ignore.

Product-wise, insurers become inspectors and start providing more microproduct watch-over services, such as with security company ADT, which offers both for home and medical alerts.[6] Products could shift from blanket to conditional coverage. For example, teen drivers could be fully covered until 9 p.m.; proof of sobriety would be required after that time. Gamification of risk-reducing behaviors and coaching applications would be bundled within such coverage, providing risk feedback as a social incentive to improve driving or health habits.

Insurers do face increased challenges in this scenario, as interface issues between disparate devices generate new risks. If edge systems remain dumb and insurers are responsible for only a portion of the interactions, emergent effects and miscommunications potentially create large liabilities. What happens when the thermostat fails and tells the water heater it's below freezing in the house? Local agents would increasingly take a role as cognitive troubleshooters for successful insurers (see Figure 5).

Survival of the fastest

Our last scenario, survival of the fastest, is generally a continuation of today's environment, with no technology gaining widespread acceptance. That does not mean that cognitive systems and distributed technologies such as the Internet of Things would fail, but rather that these technologies would be proprietary systems deployed by a limited number of participants, as opposed to common standard utilities.

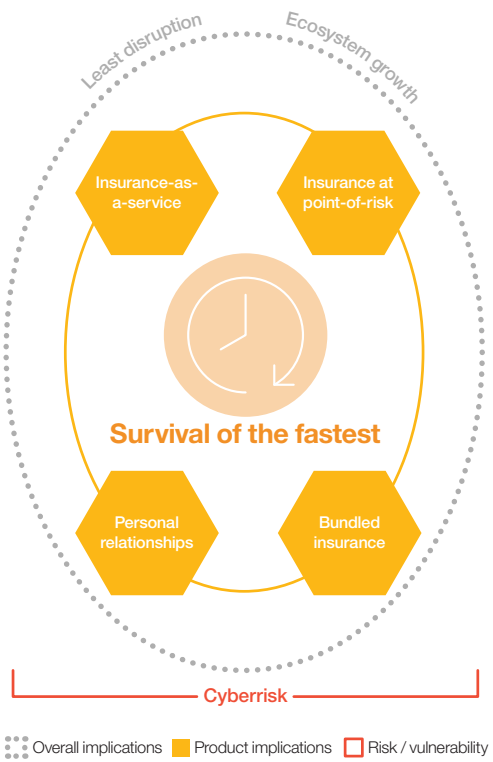
Because cognitive systems enable ingestion of a wider range of data and broader reasoning, the few organizations adopting cognitive technologies would enjoy large first-mover advantages, generally leading to further industry concentration, and, thus, survival of the fastest. These companies would strike preferred data partnerships to lock up edge data and transactions that fuel cognition, consolidating their advantage quickly.

The key "advantage" of this scenario is that it would introduce the least disruption of the current status quo. At the same time, as previously noted, the scenario is vulnerable to industry concentration, oligopolies and subsequent regulatory scrutiny.

For insurers, this scenario is potentially the most lucrative. With an undiminished high regulatory burden and little need to differentiate on product, incumbents would move to a utility industry model, relying on the range and flexibility of their distribution networks. The disruptive threat of insurtechs does not pan out in this scenario; insurtechs would go into hype curve mode, and most of these models would incur a high failure rate or be subsumed by incumbents. We are already seeing divergence in corporate venture capital funds, with weaker ones shutting down and stronger players accelerating investment.[7]

Figure 6

Insurance implications of survival of the fastest



Source: IBM Institute for Business Value

Without a broad range of insurance access to data, insurers would remain incented to drive ecosystem partnerships directly. This could enable many industries to move to maintenance-as-a-service models by bundling insurance behind the scenes with all manner of goods —we sell you hot water, not a hot-water heater.

With customer empowerment increasing and expectations rising, today's status quo — low speed-to-market and product innovation —becomes an issue. Insurers that can microsegment would have an advantage, further increasing consolidation toward cognitive and analytics adopters. Overall, there would be a strong emphasis on multi-line operation and relationships — the trust factor. Customer lifetime value becomes critical to manage, and much emphasis would be placed on trust and satisfaction measures such as net promoter score. Insurers that cannot negotiate cognitive access to distributed systems would double down on relationship and human interaction strategies to survive. Interaction frequency with buyers would become paramount, and customers will be radically empowered.

Besides classical coverage, products would expand toward insurance bundled with high-value products, insurance-as-a-service and insurance at point-of-risk. Distribution would become king, and the ability to bake insurance into other value chains and develop ecosystems would become a primary differentiator.

Some risk factors for insurers in this scenario are being "frozen out" —by regulatory changes, by lack of partnerships, by interaction frequency erosion, and by the resulting inadequate access to distribution channels. The largest, though, might be cyberrisk —currently one of the major concerns of organizations in all industries.[8] In this future, some companies —"the fastest" — would have solved these security issues, while the majority of organizations — those that do not adopt protective technologies and other measures at a fast enough rate —would be prone to fail (see Figure 6).

Preparing for the future

As we have described in the previous sections, all four scenarios are quite different, with fundamentally different implications for insurance and insurers (see Figure 7). So how can insurers prepare? Many of the technologies involved, and the business capability needs they imply, take years to develop. By the time the indicators clearly show which scenario we will be entering, it will be too late for many insurers to prepare. But preparing early costs precious investment and management attention. What to do?

Figure 7

Summary of insurance implications

	Swarm economy	Central intelligence	Internet of Everything	Survival of the fastest
Key advantage	Resilient system	Decision-making depth and microsegmentation	Market of one	Least disruption
Key vulnerability	Decision failure at the endpoints	Communications failure	Privacy	Oligopolization
Overall impact on the insurance business model	High disruption of "classical" business and distribution models	Access to information becomes paramount	Group-sales oriented, local	Highly lucrative for the fast movers; rise of ecosystems
Future insurance products and services	Microproducts, incremental helpers for health and human skills (i.e. driving, nutrition)	Holistic coverage across industry chains, zaibatsu, life and health management, insurers as agents on behalf of customers	Gamification, coaching and lifestyle management, conditional coverage, insurers as inspectors	Bundled insurance with OEM/products, insurance-as-a-service, insurance at point of risk
Risk for insurers	Local systems failure, property decay/replacement, deceit of local sensors (for example, odometer hacking), systems interference/feedback	Inadequate access to local sensors/data, reporting fraud, decision exploitation, brand reputation as "big brother"	Accusation of redlining (discrimination), miscommunication	Regulatory changes, cyberrisk, low interaction frequency, inadequate access to distribution channels

Source: IBM Institute for Business Value

We believe a set of common enablers are critical no-regret moves across all four scenarios:

Build a war chest by embracing cannibalization: Take out expenses and build in flexibility by moving to core systems with sufficiently advanced architecture: hybrid-based and cloud-ready, flexible product models that can handle a wide range of scenarios, available as-a-service to enable new market entry and experimentation at low cost, on secure and scalable platforms. As products move to "as-a-service" models, deconstructing and componentizing legacy systems will be required to sustain cost competitiveness.

Prepare partner ecosystems: Insurers will need to collaborate, both to collect data about risk and insureds and to more meaningfully participate in risk conversations. These connections will perform double duty in the future as distribution channels. Insurers need to have a seat at the table in the future, come what may in terms of market structural changes. That means cultivating partnerships and membership in ecosystems of "adjacent space" partners in relevant lines of business. Having the right partners at hand early will play a crucial role to being in the right place — close to the customer instead of in a back seat, "white label" role. With "as-a-service" products, you as insurer will often not be able to offer these alone; you will need to cooperate with manufacturers or service partners to offer the complete package. Data access and distribution access need to become core strategic drivers.

Build high-beam headlights: Slow followers will perish in any of our scenarios, but even fast followers will need to improve their speed of change – and that means knowing where you need to bring together technology, business capability and product investment. Make use of analytics and various forms of pattern recognition along with many sources of data to understand where we are on the path to the future. Understand customer behavior and risk parameters and influences at deep levels, and pursue new forms and sources of customer data.

Embrace innovation: Leading innovators build an organization that encourages innovation, create a culture that fosters innovation, and design processes that enable innovation.[9] Leaders can be proactive because they have created structural flexibility that makes taking quick, early action self-reinforcing. Start by streamlining internal innovation processes, with central funding and investment models and quick-hit projects and partnerships. Embracing innovation will build skill with component technologies of whichever future scenario wins, providing the capabilities necessary to prosper in changing conditions. And building agile development and business service composition skills will keep your organization nimble enough to capitalize on market changes.

For more information
To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for your phone or tablet from your app store.

The right partner for a changing world
At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value
The IBM Institute for Business Value, part of IBM Global Business Services, develops fact-based strategic insights for senior business executives around critical public and private sector issues.

Are you ready for the insurance world of 2025?

To what degree has your organization adopted cognitive technologies? How are you utilizing decentralized technologies such as the Internet of Things and blockchain?

Which products and services , besides classical coverage of risk, are you considering? What are the impediments to doing so?

How are you partnering and collaborating to build ecosystems? If you aren't, why not?

Do you have early warning indicators to recognize which future we are headed into? What are they? How are you building the skills of your workforce to cope with the future you identify?

About the authors

Christian Bieck is the global insurance leader for the IBM Institute for Business Value. He is an economist by training, and he worked in various roles in the insurance industry in Europe before joining IBM as a process consultant and researcher. Christian is a frequent speaker on thought leadership and innovation at insurance events and workshops. He has authored various papers on insurance trends and implications, both for the IBM Institute for Business Value and international insurance industry publications. Christian can be reached at christian.bieck@de.ibm.com.

Mark McLaughlin is IBM's Global Insurance Director. Mark leads the IBM Global Insurance team in predicting industry business and technology trends, leveraging those insights for the world's largest insurers and developing IBM solutions in the insurance vertical. Mark directs IBM strategic collaborations with senior industry leaders, bringing IBM's experience and innovation together to build sustainable competitive advantage for insurers. Mark previously has led business units in insurance distribution and analytics, technology infrastructure, CRM and insurance business process, and has led projects at multiple top 20 U.S. insurers. He is a 20-plus year veteran of the insurance industry. He can be contacted at mmclau@us.ibm.com.

Contributors and acknowledgments
The authors would like to thank the following individuals for their contributions: April Harris, Jim Phillips and Anupama Shukla for their work on the executive report; the cyberrisk study project team of Swiss Re (Philippe Aerni, Jonathan Anchen, Dr. Maja Bundt, Eric Durand, Roman Lechner, Darren Pain and Michael Schmitt) for their contribution to the development of the 2025 scenarios.

Notes and sources

1 K. K. Steincke, K.K. “Farvel Og Tak: Minder Og Meninger”. p. 227. Forlaget Fremad, København., Copenhagen, Denmark. 1948

2 “Redefining Boundaries: The Global C-suite Study.” IBM Institute for Business Value. November 2015. http://www.ibm.com/services/c-suite/study/study/

3 Pureswaran, Veena and Paul Brody. “Device democracy: Saving the future of the Internet of Things.” IBM Institute for Business Value. September 2014. http://ibm.biz/devicedemocracy

4 Bieck, Christian, Andrea Cornelius, Sandip Patel and Hirosuke Uramatsu.“Rethinking insurance: How cognitive computing enhances engagement and efficiency“. IBM Institute for Business Value. December 2016. http://ibm.biz/rethinkinsurance

5 IBM Institute for Business Value analysis, based on publicly available information

6 ADT. http://www.adt.com

7 Pash, Cris. “AMP’s startup venture fund is gone.” Business Insider Australia. January 25, 2017. http://www.businessinsider.com.au/amps-startup-venture-fund-is-gone-2017-1

8 Bieck, Christian, Maya Bundt, Patricia Hamilton, Kurt Karl, Michael Schmitt and Pawel Stefanski. “Cyber and beyond: Insurance and risk in a digitally connected world.” IBM Institute for Business Value. June 2016. http://ibm.biz/cyberinsurance

9 Bieck, Christian, Lynn Kesterson-Townes, Anthony Marshall and Indranil Nath. “Innovating insurance – Lessons from the world’s leading innovators.” IBM Institute for Business Value. March 2016. http://www-935.ibm.com/services/us/gbs/thoughtleadership/innovatinginsurance/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
March 2017

GBE03821USEN-01