Opportunities through the Internet of Things: From Claims Management to Claims Prevention

Jörg Thews

Jochen Schlicksupp

The pace of technological change and increasing customer demands have led to a new wave of competition that many insurance companies find threatening. Although the current wave of technology investments has mainly focussed on improving the customer experience and reducing costs, it is now shifting to new business models. The increasing use of sensors in combination with Artificial Intelligence (AI) has affected the practices of loss anticipation and compensation, moving them towards more proactive risk detection, intervention and prevention. This environment brings opportunities for the insurance industry to develop new products, open new distribution channels, and extend its role to include prediction, prevention as well as assistance (PwC, 2019).

IoT: A New Ecosystem of Information

The Internet of Things (IoT) hype continues unabated: Gartner predicts there will be 20 billion networked devices by 2020 (vs. 8.4 billion in 2017); IDC estimates IoT expenditures of USD 1.2 billion by 2022; analysts forecast potential IoT sales of EUR 50 billion for Germany in 2020 (PwC, 2020). The industry association Bitkom ranks IoT among the top three trends in the information and communications technology (ICT) sector.

Opportunities for the Insurance Industry

From car sensors to smart homes or wearables like fitness trackers, IoT has entered customers' everyday lives and is transforming the physical objects that surround us into an ecosystem of information. This new ecosystem of information will generate expansive economic growth by transforming business models, unleashing innovative products and services. Insurance companies can use the data collected from the business environment to achieve enhanced process optimization and efficiencies. Moreover, now that more and more businesses are adding sensors to people, places, processes and products to gather and analyze information, it allows insurance companies to improve operations, redefine consumer relationships, and create entirely new revenue streams. Market experiences and adoption cases in the motor insurance market show that insurers can reduce the claims frequency of motor third party liability insurance (MTPL) by around 20 percent (PwC, 2016a). Connected home insurance is expected to decrease potential losses by 40 percent (PwC, 2016a).

Challenges for the Insurance Industry

Cyber security and data privacy are currently the main challenges for the implementation of IoT solutions. In fact, there is no global guideline or agreement which regulates who is responsible for a platform's security. Unlike IT equipment, connected devices were not designed with security concerns in mind which causes additional security risks. HP Fortify on Demand reviewed ten of the most commonly used connected devices and found that 70 percent of them show serious vulnerabilities (PwC, 2017). Addressing these shortcomings will be a hurdle because many devices lack the computing power to handle essential technologies like encryption, web interface, authentication and automated patching.

At the other end of the spectrum, once powerful legacy systems are not updated because they may be at the end of their life cycle. They may also be incapable of

The authors

Jörg Thews is Partner at PwC Switzerland, where he leads the division Insurance Practice.

Jochen Schlicksupp is Director at PwC Switzerland, where he leads the division Insurance Technology Services.

64 %
of CEOs believe technology will disrupt how they do business in the next five years.

73 %
of global companies invest in IoT and value it as the top priority technology in the next years.

47 %
of decision-makers say IoT is becoming the key technology for efficiency increases and cost optimizations.

Fig. 1: IoT is driving the digital transformation. (Source: PwC, 2020)

interoperation with disparate new systems, software and communication protocols (PwC, 2017).

From a technological point of view, the key to success is optimally handling the complex data collected from countless networked objects and «integrating» them quickly and flexibly using suitable platforms. But technological approaches alone are not enough. In order to successfully leverage IoT, the business model has to change fundamentally. This change requires:

- A new value proposition and a new value chain in which the insurance company acts as an integrator for different industries
- New partners with specific competencies (processes, management of systems and data etc.)
- New distribution channels tailored to the newly developed products and services
- Suitable operational and organizational structures to be able to scale

Connected Insurance: Towards a New Insurance Business Model

Connected Insurance, as an evolution of the insurance business model, is primarily enabled by IoT technologies that allow the direct interaction of all actors of this information ecosystem: customers, insurers, technology providers, and players from other industries. Three different digital ecosystems are emerging that are most relevant and attractive for insurers: connected car, smart home and connected health. Although these ecosystems certainly have parallels, insurance companies have to develop an individual strategy for each of these ecosystems to address the differences appropriately. The degree of market maturity differs in each of the ecosystems, and they feature some clear distinctions in terms of market dynamics, relevant players and regulatory environment.

Connected Car

Connected cars enable internet connectivity, blind spot monitoring, real-time navigation, lane departure warnings and vehicle diagnostics. Insurers can use this technology to improve their risk monitoring and to accurately price risks. Moreover, using the collected data for claims prevention (e. g., warning a driver, if he or she is driving too fast) enables the insurers to create new value propositions as a prevention service provider. In addition, the claims handling can be automated to a certain degree such that claims handlers only have to review special insurance claims. Moreover, it is easier to identify suspicious behavior such that insurance companies can detect insurance fraud more effectively.

Due to the increased usage of the abovementioned IoT technologies, a new ecosystem is emerging around the automobile. It includes, for example, sensor manufacturers, research institutes, garages, towing services and insurers. This ecosystem alters the competitive parameters for all participants – in particular, insurers. Various insurers worldwide have already partnered with IoT-based telematics suppliers, automotive original equipment manufacturers (OEMs), vehicle repair shops, telecom companies and system operators that guide drivers to free parking spaces. Such partnerships will provide both sides with access to the valuable sensor data that will lay the groundwork for new hybrid insurance models.

Smart Home

New smart devices are embedding insurers in people's homes, enabling policyholders to benefit from real-time equipment monitoring and maintenance. This connectivity is strengthening policyholders' trust, which is central to the insurance business (PwC, 2019). Customers engage more frequently with smart home apps which generate a huge amount of data about homes. Insurers can use this data to provide their customers with information about the risks they are exposed to such that the home owners can monitor how those risks progress. Moreover, insurance companies can use their competence in risk management to show home owners how they can mitigate the revealed risks. So, smart home devices are promoting safer behavior by building greater risk awareness. This safer behaviors may also be rewarded by insurance companies. As a result, many insurers around the world (e. g., Allianz) have started cooperation models. They sell integrated products via Google Nest or offer insurance discounts for people who equip their homes with smart home devices. In addition, insurers offer digital add-on services such as home security and convenience services (e. g., Liberty Mutual).

Connected Health

To track the customers' health behavior, activities and habits, insurance companies incorporate sensor-based monitoring solutions such as biosensors, wearables and mobile apps into their insurance products. With the help of analytical tools applied to aggregated data, insurers determine which clinical processes may have the better impact on a patient's health. IoT allows insurers to provide additional services such as telemedicine and virtual visits. The customer can benefit from a premium reduction or a reward for good behavior (Pay-As-You-Live). The collected data is at the heart of personalization and is critical for tapping into the arising business opportunities. Benefits accure from personalized offers, better customer management and im-

proved decision making. At the moment, new players, such as the new healthcare venture Haven, are disrupting the market. Haven was established by Amazon, Berkshire Hathaway and JPMorgan Chase with the vision to create better outcomes, greater satisfaction and lower costs for their US employees and families. Currently, the Covid-19 pandemic opens up new opportunities and applications, such as the app from the Robert Koch Institute (RKI) in Germany which should help to better understand how Covid-19 spreads in Germany.

Tackling the Cyber Security and Data Privacy Challenges

The opportunities for Connected Insurance are too compelling to ignore. Insurers see the emerging platform as a catalyst for change, a vehicle to boost competitive advantages, increase operational efficiencies and create new revenue streams. But the lack of IoT standards and guidance represents a significant obstacle. To overcome this obstacle, businesses can follow existing best practices that will help building a strong foundation for IoT cyber security. An IoT cyber security initiative should begin with a careful assessment of all data across the business ecosystem – including the extended IoT platform, third-party partners and communications networks. Organizations will need a solid understanding of the value of data, the number and type of data assets, where data is located and transmitted, who has access to this information and the potential impacts of data breaches.

The use of personal information should be limited to the specific purposes for which it is collected. The notion of «privacy by design» was viewed as a best practice but is now mandatory under the General Data Protection Regulation (GDPR). In order to meet the GDPR requirements, organizations have to make sure that applications only use the personal information that is truly necessary for a product or service to work. Moreover, multinational businesses will need to implement processes to ensure that the transfer of personally identifiable information across borders does not violate data protection laws. Doing so will require an up-to-the-minute understanding of data privacy regulations across different locations and knowledge of emerging interpretations on the ethical use of information. Going beyond GDPR, businesses should work carefully with legal and compliance stakeholders to ensure they implement appropriate privacy safeguards.

Beyond data, it will be integral to regularly assess the security capabilities of connected devices. As the IoT platform matures and connected devices proliferate, it is unlikely that businesses will be able to evaluate all connected equipment – but they should identify, inventory and evaluate the security capabilities of critical at-risk equipment. The assessment should be performed at the network, application, data and physical layers, and includes ethical hacking as well as vulnerability testing to understand the weaknesses of connected devices and how hackers might exploit them. Moreover, businesses should carefully assess potential vulnerabilities in entry points between services and devices. Cyber criminals often take advantage of weaknesses in Application Programming Interfaces (APIs) between mobile devices, web interfaces and cloud systems to gain a foothold into IT systems (PwC, 2017).

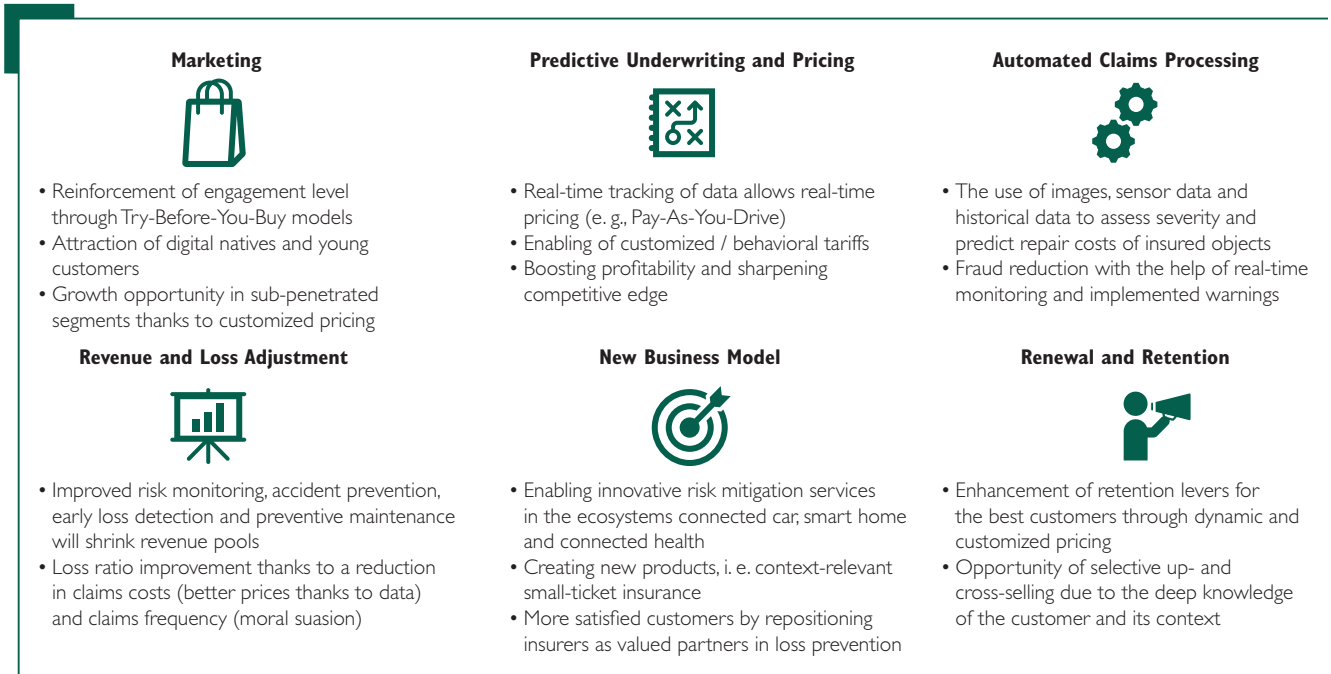

Fig. 2: IoT is disrupting the entire value chain of insurance companies.

Internet of Things: More than a Buzz Word

IoT is not only the industry's buzz word but can also prove to be very efficient in generating insights from external data sources. Ongoing initiatives are reaching significant benefits along the entire value chain and open up new opportunities for the insurers (see Figure 2).

In order to use IoT's full potential, insurance companies need to extend their offerings through non-insurance services, cross-industry collaborations and partnerships to develop an enhanced customer engagement model which prevents claims and rewards good behavior. At the same time, insurers have to invest more heavily in data and cyber security.

To successfully leverage IoT business opportunities, insurance companies need a clear and consistent IoT strategy which answers the following key questions:

- What role do you want the company to play in the IoT sector?
- Why do you want IoT to be used in the company?
- What IoT capabilities are required for success and how will they be established?
- What are the next steps to launch IoT in the company?

In summary, IoT undoubtedly makes losses easier to predict and prevent. Smart home devices, wearables and driverless cars will lead to a shift towards a new type of customer relationship where insurance becomes less reactive and more preventative.

References

PwC. (2016a). Connected Insurance: Our View about the Italian Market. Retrieved from: www.pwc.com/it/it/publications/assets/docs/connected-insurance.pdf.

PwC. (2016b). Megatrend Financial Center: Insurer 4.0: Turning Change into an Opportunity. Retrieved from: www.pwc.ch/de/publications/ 2016/tp_versicherer_4-0_en_web.pdf.

PwC. (2016c). Opportunities await: How Insurtech is reshaping insurance. Global FinTech Survey June 2016. Retrieved from: www.pwc.com/gx/en/financial-services/assets/fintech-insurance-report.pdf.

PwC. (2016d). The Wearable Life 2.0: Connected Living in a Wearable World. Retrieved from: www.pwc.se/sv/pdf-reports/the-wearable-life-2-0.pdf.

PwC. (2017). Uncovering the Potential of the Internet of Things: Key Findings from the Global State of Information Security Survey 2017. Retrieved from: www.pwc.com/gx/en/issues/assets /pwc-GSISS-2017-uncovering-the-potential-of-iot.pdf.

PwC. (2019). Insurance Trends 2019: Digital Transformation Shifts from Threat to Opportunity. Retrieved from: www.pwc.ch/en/publications/2019/PwC_2019_CEO_InsuranceReport_Final.pdf.

PwC. (2020). IoT is Driving the Digital Transformation. Retrieved from: www.pwc.de/en/digitale-transformation/internet-of-things.html.