No.1 Cornhill, City of London EC3V 3ND
020 7060 4090 - ninety.co.uk

A Ninety Consulting white paper

The Connected Home

What does this mean for insurers now and in years to come?

By Dan White and Geoff Knott

Background

Insurers have already become familiar with smart devices in cars and have used telematics capabilities to create more accurate risk profiles leading to personalised policies that reflect actual car usage and how the car has been driven.

This telematics risk profiling approach will only increase - in the USA, after Sept 1st 2014, event data recorders will be mandatory in all new vehicles[1], with most Western societies implementing similar legislation.

And now, smart devices are set to penetrate the home market. These are making inroads through popular consumer solutions. As smart home technology evolves, insurers may have the opportunity to use real-time telemetric data for the assessment of risk and prevention of loss.

Before we try to predict what this might mean for an insurer, let's look at some of the technology.

Connecting the unconnected

Connected devices in the home are just one part of the move towards 'the Internet of Everything'. At its advent, people drove the Internet – human beings entered and shared information. Now smart devices like phones capture and share information about us. With 'the Internet of Everything', connected things add powerful new capabilities like contextual awareness, increased processing power but, critically, an ability to send data to one or more cloud services. This added information gathering and sharing will allow for faster, more intelligent decision-making by people and machines. Cisco estimate that 37 billion new things will be connected to the internet by 2020[2].

The connected home market is breaking out from niche solutions for the wealthy, e.g. monitored security systems, to the mass market.

Focusing on the connected home segment, various brands are competing to become the standard, the technology of choice, not only for devices around the home but also the communication method between devices. Both Google[3] and Apple[4] have recently moved aggressively into this space. The market is in an early adoption phase and it is unclear which brands will win out. The market is breaking out from niche solutions for the wealthy, e.g. monitored security systems, to the mass market.

However, some things are clear - the success of the smartphone/smart TV has created a natural interface for customers to interact with their devices; Wi-Fi/broadband in the home allows devices to communicate with each other and externally; and there are some common applications which are emerging.

These common applications can be summarised as:

- Intruder alarms – detects intrusion, calls contacts, takes pictures, etc.
- Thermostats - senses routines of residents and controls equipment accordingly.
- Lighting - allows control of individual lights from an app and sets away-from-home schedules.
- Smoke/CO detectors - notifies householder and closes down heating, ovens, etc.
- Refrigerator - alerts to power outages or if a door is left ajar.
- Oven - preheats the oven based on calculating time of arrival home, sets the timer, and checks cooking status without being in the room.

- Electronic door locks - remotely locks or unlocks and changes who is authorised to enter. Includes fingerprint scanning and other recognition software. They can also keep homeowners informed about who is entering and leaving the home, when they left, how long they were there, etc.
- Water alarm - texts when water detected from tanks, appliances, etc. Shuts off water supply.
- Washer/dryer - starts cycles and monitors progress, alerts to problems.

Some applications that could emerge in the future include:

- Conditions the home is exposed to - temperature, wind speed, humidity and mechanical vibrations.
- Groundwater levels – currently water leak detectors could be placed in basements for early detection of floods. This could be extended to undersoil groundwater monitoring.
- Food stocks - refrigerators that know what food is stored and can reorder. Use of healthy food can be tracked.

In addition, as smart devices get built into appliances, they will be able to self-check status, allow remote maintenance diagnostics and call an engineer to make an appointment, preventing costly damage before it happens.

These devices will all need to be able to 'talk' to each other. A smoke alarm will need to talk to the fuel supply or the central heating boiler, the oven, the fire, etc., and command them to close down (doing so 'smartly', so as to avoid false positives).

Several companies have recently demonstrated progress in getting smart home devices from different manufacturers to link up and work together. However, other companies e.g. Samsung plan to go it alone, releasing ranges of smart home gadgets only compatible with each other but allowing other companies to programme their own gadgets to work with that system. Consumers could end up with several apps to control their home and that could lead to some frustration. In addition, connecting anything to a secure home Wi-Fi network is a challenge for many. Differential access will also be critical for the wide range of formal and informal arrangements that households require – family members, cleaners, etc.

Therefore, there is a distinct difference between car and home telematics. With a car, there is only one box with a simple range of metrics. With a home, there will be many devices, from different brands, with a wide range of metrics. The costs of collecting such data could be a stumbling block (as, indeed, could the cost of providing and fitting the necessary equipment).

A viable approach for an insurer could be to enter this emerging market niche by niche, e.g. security applications first, smoke alarms next, etc. It may also be necessary to have the consumer carry much of the up-front purchase and installation cost, though this can be double-subsidised; once through partnerships with technology providers, and once through discounted premiums.

There is a distinct difference between car and home telematics. With a car, there is only one box with a simple range of metrics. With a home, there will be many devices, from different brands, with a wide range of metrics.

Consumer research

The availability of new technology means nothing if consumers do not embrace it. And so what of the consumer?

A UK survey[5] in May 2014 by Npower found that 46% of Britons believe that the use of remote devices around the home, such as smartphones to control appliances, is a positive thing. In fact, one in 10 said they couldn't live without these gadgets. The survey of 2,000 UK residents found that 22% said they found using remote devices saved them time, while 10% said it had saved them money.

A USA State of the Smart Home Report[6] in May 2014 based on data from more than 900 U.S. adults, found that:

- 86% ranked property loss protection as a top reason for a smart home system
- 78% of consumers ranked energy management as one of the top features that matter most in the smart home
- 67% ranked personal and family security as the number one reason for using a smart home system
- 52% of pet owners listed pet monitoring as one of the top five most important reasons for using a smart home service

A 2013 report[7] from Berg Insight estimates that North America is the most advanced region in the world for smart home solutions with an installed base of 3.5 million systems at the end of 2012. An estimated 0.7 million of these were multifunction or whole-home systems whereas 2.8 million were point solutions designed for one specific function such as climate control or security. As some homes have more than one smart system in use, the installed base represents a total of around 2.9 million smart homes. Market growth was very strong during the first three quarters of 2013 and North America was on track to reach an installed base of 5.5 million smart home systems by the end of 2013. Between 2012 and 2017 the installed base is forecasted to grow at a compound annual growth rate of 55.0 percent to reach 31.4 million smart home systems.

The European market for smart home systems is still in an early stage and approximately three years behind North America in terms of penetration and market maturity. At the end of 2012, there was a total of 1.06 million smart home systems in use in the EU27+2 countries. Around 0.15 million of these systems were multifunction or whole-home systems whereas 0.91 million were point solutions. This corresponds to around 0.93 million smart homes when overlaps are taken into account. Market growth was solid during the first three quarters of 2013 and Europe was on track to reach 1.45 million smart home systems by the end of the year. Berg Insight's 2013 research[8] forecasts that the installed base of smart home systems in EU27+2 will grow at a compound annual growth rate of 56.0 percent in the next five years to reach 17.4 million systems by 2017.

Consumer benefits and risks created by the technology

The main benefits for the consumer are seen as:

- Energy efficiency – turning devices on/off only when needed, only heating the home when it is occupied.
- Increased security – detecting intrusion, switching on/off appliances to make it appear someone is in the house.
- Convenience and comfort – being able to save time and activate devices before home arrival. Being able to check on the home remotely.
- Incident prevention – not only by early warning and shutting down of systems in an emergency but also in detecting the need for maintenance.
- Saving money due to preventative actions above.

With all new technology, there are risks and these are seen as:

- Hacking - each device added to the network needs good security settings otherwise hackers could access connected products in your home. Firewall software is already being marketed for manufacturers to embed into their smart devices[9].
- Data privacy – devices can show when you are away from home, or your house to/from work pattern. Systems collecting this data need to be secure.
- Redundant technology/ lack of standards - as has been said, connectivity is still in its infancy, with no clear winner among competing technologies. The embedded technology may become redundant and may not work well or at all with other devices.
- A single point of failure - the smartphone will become a mission-critical piece of equipment in our everyday lives. Lose your phone and lose access to devices.

Know your customer

We know that smart homes are and will become a reality. What matters for insurers is to look at how information collected by the devices can be used to assess risk and therefore premium levels, as well as minimise claims levels and fraud risk.

Whilst there are no concrete predictions of risk reduction levels resulting from use of these technologies, Allstate in the USA offer a 25% discount off home insurance for users of security applications, and State Farm offer a 10% discount.

The common applications of smart home technology provide data for three main risk areas which drive big ticket claims:

- Burglary
- Fire
- Water leaks

Preventing damage: first and foremost, the new devices are designed not only to prevent damage but also contain and limit it. This will create a significant impact. In homes where all common sources of potential water leaks were actively monitored and could interrupt the water supply, water damage claims would very seldom occur.

Lifestyle monitoring: beyond this critical and most fundamental impact, data from these new devices will be able to be analysed to provide information on home lifestyle and maintenance patterns which could increase or decrease risk, e.g. time away from home, use of water, boiler servicing, etc.. Insurers will be able to proactively recommend changes to lifestyle to help their customers better protect their homes.

Fraud detection: so long as data privacy issues can be resolved, data from connected homes will be able to detect or deter potential frauds – e.g. claiming accidental damage when no-one was at home.

Structural stress assessment: once devices exist and are built into houses that monitor conditions the home is exposed to, e.g. temperature, wind speed, humidity and mechanical vibrations, then risk to the exterior fabric of the home can be assessed more accurately.

All of these new avenues are gradually being opened up to insurers, giving an opportunity not only to create a more personalised quote for a prospective customer based on the ability to identify high and low risk homes, but also the potential to reduce risk overall and to more intelligently manage remaining claims. In all this, clearly, insurers will face a second tide of data (motor telematics having been the first), and this will be a challenge which will increase the pace at which they embrace cloud technology providers, who are more natively able to handle such challenges.

Actions by insurers to date

The connected home, and its impact on insurance, are not things of the future: several insurers have already offered products in this segment, working with specialist partners in each case:

In May 2012, Allstate Canada teamed up with Rogers, a supplier of Smart Home Monitoring equipment to offer a 25% discount on their home insurance premium[10]. Allstate customers also receive a free water leak sensor from Rogers as part of an exclusive hardware package that also includes an easy-to-use touchpad, three window and door sensors and a motion detector.

At the end of 2013, in the USA, State Farm and ADT partnered to provide the home security company's home-monitoring technology, ADT Pulse, to State Farm policyholders[11]. Signing up for the service provides discounted installation, lower monthly service fees and more competitive insurance premiums. At the same time, State Farm also extended discounts to users of IRIS home security products from Lowe's, the DIY chain[12].

Also in late 2013, BNP Paribas in Italy launched Habit@t[13], the first home insurance product "that you can touch": a fully packaged home security telematics device that protects and monitors the home for perils such as fire, smoke and flooding, and alerts both the customer and an operation centre, which immediately activates an assistance service. The policy, thus, is not merely one that provides financial compensation, but true protection.

In June 2014, Allianz and Deutsche Telekom announced they are combining their respective market solutions to offer what they called "connected life" services[14]. Leveraging Telekom's communication infrastructure both businesses said they are developing a connected home service package for the European market. Connected life will be the combination of Telekom's "Smart Home" solution and "Allianz Assist" emergency assistance service for the home.

Thus different insurance services are being affected – not only home insurance, but also emergency assistance, which will make a lot of sense to customers.

Apart from DIY adopters, partners will be key to opening up this market for insurers. Partners such as energy and utility companies, or security services, have a network of installers and they do regular home visits. If an insurer wanted to develop a direct service, the cost of devices and of installation are high relative to the insurers' premium income and the logistics would be complicated for an insurer to manage. Energy and utility companies with home maintenance, household insurance offerings and smart home technologies (e.g. British Gas and their HomeCare and Hive products) may find themselves in prime position to benefit.

Partners will be key to opening up this market for insurers.

Early days but still a long way to go

Initial actions by insurers have focused on partnerships with technology providers based on the premise that consumers who use such equipment are a lower risk. In effect the policyholder is perceived as a

better risk manager. They are securing their home, thus helping prevent burglary. If an incident such as a water leak happens, they can shut off water flows, etc.

The policyholder of a smart home is perceived as a better risk manager. They are securing their home, thus helping prevent burglary. If an incident such as a water leak happens, they can shut off water flows, etc.

There is obviously a sales opportunity to customers who buy such equipment, thus opening up a new market for insurers. But there is also a marketing opportunity for insurers to make their existing customers aware of lower premiums if they install a partner's devices (with the insurer benefiting, in aggregate at least, from lower claims).

The next logical step will be to move beyond knowing that devices are in place, to monitoring the data from such devices. This would be similar to telematics from cars. Private information will be expected in order to offer a premium discount. There will be a move to usage-based insurance (UBI) as insurers use behaviour-based telematics to supplement traditional underwriting factors in the home.

Premium discounts will not just depend on knowing a device is there, but on actual intelligence from the device, i.e. have the doors been locked, has the alarm been set, has the boiler had a service, are the batteries in a smoke alarm charged, etc.

Beyond that, insurers will also monitor use of the house to see if certain behaviours lead to increased risk, e.g. leaving the house empty for long periods or predictable periods, letting temperature in the home fall low, multiple people using the home, etc.

The monthly premium charged will in some cases become a variable figure, based on behaviour that month and perceived risk incurred. This will incentivise the homeowner to modify home use, as has happened with car telematics.

In order to offer these products and services, either device data will need to become 'open' so that any insurer can use it, or insurers will need to forge strategic partnerships with major players in the connected home arena. If the former, customer loyalty and switching will be an issue. If the latter, picking the right partner will become key, but this could also lead to accusations of customer lock-in and anti-competitive practices.

In the end, to ensure the broadest possibility of return on investment, insurers will need to develop interfaces to devices from various manufacturers in order to aggregate the data for risk analysis. Rather than every insurer trying to do this, there is an opportunity for an aggregation service, paid for by a group of insurers, to collect the data from a customer, analyse for risk and present back to the customer's insurer. This aggregator can also deal collectively with data privacy issues with regulators.

Premium discounts will not just depend on knowing a device is there, but on actual intelligence from the device, i.e. have the doors been locked, has the boiler had a service, are the batteries in a smoke alarm charged, etc.

As well as predicting risk, the data will be used by more pro-active insurers through CRM systems to open up other opportunities for insurance, e.g. equipment failure and replacement, telematics-based car insurance, and more.

If they have not already done so, insurance companies should be including actions on this emerging market in their strategic plans, exploring partnership routes, considering effects on IT systems, and more, but - most of all - deciding how to benefit customers who take advantage of connected homes

technology.

- END -

ABOUT NINETY CONSULTING

At Ninety Consulting we design digital strategies and build roadmaps, particularly for the General Insurance sector. We turn opportunities into fresh, engaging, relevant digital formulas. Digital formulas that inspire. Empower. Deliver. Turn complexity into simplicity. Ambitions into deliverables. Visitors into customers. Our consultants have driven digital strategy for most of the major insurers in the UK: Aviva, Direct Line, LV=, MORE TH>N, Allianz, Legal & General, Hiscox, Zurich, Admiral, the Co-operative Insurance and more. See http://ninety.co.uk for more on what we think and do.

To discuss any part of this report, or to have us help you consider the implications of the connected home on your insurance business, contact Dan White, Senior Partner for General Insurance, on dan.white@ninety.co.uk or 020 7060 4090.

REFERENCES

[1] http://www.gpo.gov/fdsys/pkg/FR-2012-12-13/pdf/2012-30082.pdf
[2] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.html
[3] http://venturebeat.com/2014/01/13/google-buys-nest-for-3-2b-its-key-to-the-connected-home/
[4] https://www.apple.com/pr/library/2014/06/02Apple-Releases-iOS-8-SDK-With-Over-4-000-New-APIs.html
[5] http://www.talktalk.co.uk/news/technology/article/future-lies-in-remote-control-homes/129986/
[6] http://www.icontrol.com/press-releases/new-research-examines-smart-home-adoption-drivers-and-outlook-for-a-connected-future/
[7] http://www.berginsight.com/ReportPDF/ProductSheet/bi-sh2-ps.pdf
[8] http://www.berginsight.com/ReportPDF/ProductSheet/bi-sh2-ps.pdf
[9] http://www.iconlabs.com/products/floodgate-at-home/
[10] http://www.newswire.ca/en/story/982139/allstate-canada-launches-new-program-with-smart-home-monitoring-from-rogers
[11] http://online.wsj.com/article/PR-CO-20131203-905985.html
[12] http://industryedge.nationalhardwareshow.com/2013/12/lowes-partners-with-state-farm-for-home-management-system
[13] https://www.youtube.com/watch?v=dbmo1oo743M
[14] http://www.connectedhomeworld.com/content/allianz-insurance-wants-connected-home-market

NINETY