IoT: Insurance, Opportunities, Threats

Molly Belmont

Junior

Temple University

Storm Wilkins, JD, CPCU

Ten years from now, a family of four could own 100 connected devices, only a small fraction of the 30 billion devices (6% of the global economy) there will be worldwide (Reifel, Pei, Lala, & Bhardwaj, 2015). All of these connected devices are designed to easily communicate data with the consumer and are part of a greater network called the Internet of Things (IoT). From trash cans that can alert sanitation crews when they are full to increase efficiency to cars that track driving for discounted auto insurance, the Internet of Things is "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or external environment" (Gartner). As customers quickly incorporate these products into their everyday lives, insurers are faced with opportunities and challenges to manage the data and the exposures. The Internet of Things is a rapidly growing network that is just beginning to flood the insurance industry with greater access to predictive data. The increased connectivity opens a number of doors to better predict and prevent losses, however as the network expands the threat of cyber risk does as well.

The insurance industry has been presented with a unique possibility to harness easily accessible data and use it for better underwriting and education of their customers. Many insurers have already begun to take advantage of the Internet of Things, but if insurers are not proactive they could get lost in the shuffle.

Partnerships are one way many insurers are embracing the Internet of Things. In June 2015, Google Nest, providing connected smoke detectors, thermostats, and alarm systems, partnered with Liberty Mutual and American Family Insurance offering discounts costs for Nest products and lower monthly homeowner's insurance to policyholders using the products (CBInsights, 2015). Censio and Progressive partnered in September 2015 to create a driving program that monitors cell phone usage while driving as well as other habits of drivers. Progressive uses the data it receives from the Censio device to offer lower rates to low risk drivers (CBInsights, 2015). Offering lower premiums, discounts, and rewards to customers based on data received from the IoT is known as Usage Based Insurance (UBI). Thus far, auto insurance has been the most utilized area of UBI.

In 2013 when UBI auto insurance was beginning to hit the test market, Towers Watson received overwhelmingly positive feedback about consumer's interest in participating in the program. They were not only interested in lower premiums and discounts, but the value added features like theft tracking, emergency response, and vehicle wellness reports (Wozman, 2013). The feedback reveals the possibilities insurers have to expand connectivity past lower premiums. John Greenough, a researcher for Business Insider Intelligence, predicts 17 million drivers have participated in UBI auto insurance by the end of 2015 and over 50 million by the end of 2020 (Greenough, 2015). This responsiveness from consumers and insurers is because of the mutual benefits they receive. Many insurers offer lower rates for people who drive less frequently and who drive safer, benefiting the customer. In addition, less frequent, more careful drivers lead to less "accidents, congestion, and vehicle emissions, which benefits society" and the insurers in turn receive less claims (NAIC, 2015). As consumers become more comfortable with UBI, the utilization of the Internet of Things will grow. Entrepreneurs and insurers are already working together to create connected devices to increase access to data and safety.

In the past insurance has been seen as a stagnant industry, however as technology and innovation have changed how the marketplace operates, insurance has proven an adaptable, creative industry. The insurance industry's proactive reaction to the IoT has perpetuated their adaptable image. Right now the most prevalent devices in the IoT are wearables like the FitBit and Google Glass, UBI in cars, and smart home devices like Google Nest. As discussed earlier, insurers have already penetrated these markets to reward low risk customers with discounted costs and access to progressive technology programs and products. However, what is more incredible is the expansion of the IoT and the partnerships insurers have already formed to add new connected products to the network. The IoT is allowing for new safety possibilities that were inconceivable before. After the success of programs like UBI for drivers, it was clear that the IoT had untapped potential that insurers should begin to explore.

Entrepreneurs and insurers are working together to leverage the potential of the IoT, specifically in high-risk areas that affect three major divisions: the connected car, the connected self, and the connected home. We saw how insurers are using UBI in the connected car. The connected self has been utilized extensively by health and life insurers using wearables to reward their customers for healthy behaviors, but even from a property and casualty standpoint the connected self can still be utilized. Workers compensation is a high risk, compulsory area of property and casualty insurance. The claims from worker's compensation losses often have a long tail and are costly. Insurers and entrepreneurs saw this problem as an opportunity to utilize the IoT to create a solution to an age old problem. In 2014, 4,679 workers were killed in job related accidents of which 1 in 5 were construction workers (OSHA, 2014). Recently AIG, "one of the world's largest worker's compensation insurers", announced an investment in a startup company working to create workplace wearables (Simpson, 2016). The company, Human Condition Safety, plans to combine "wearable devices, artificial intelligence, building information modeling, and cloud computing" to prevent workplace injuries and fatalities. The CEO of Human Condition Safety, Peter E. Raymond remarked,

> "It's not acceptable that we can push a button and have anything in the world delivered to our doorstep, but that people can still get hurt and even die needlessly when they go to work. With HCS' tools, we leverage technology to keep people healthy and safe (Simpson, 2016)."

AIG's strategic investment in Human Condition Safety represents an ongoing commitment to using the IoT to improve workplace conditions and lower worker's compensation costs. Rob Schimek, AIG's Commercial Insurance CEO, expressed that this partnership is only the beginning. AIG will continue to look for entrepreneurial companies, like Human Condition Safety, that are employing use of the IoT (Simpson, 2016). AIG is a great example of a company embracing change and adapting to the IoT's connected self.

Similarly, a few insurance companies are investing in Smart Home companies to encourage their homeowner's insurance policyholders to maintain safe living practices.

According to Fortune Magazine, consumers did not gravitate toward the Smart Home appliances like manufacturing companies were hoping. The average customer could not see the benefit of an expensive, connected thermostat or other devices (Higginbotham, 2015). Insurers, however, could see the benefit of a slightly more expensive thermostat or a carpet that alerts of any unauthorized foot traffic and have been investing in the Smart Home appliances in hopes of offering discounts to their policyholders who use them in their homes. State Farm is one of the leading forces with IoT Smart Home devices partnering with Canary, an all in one Smart Home security system. Canary gives users the ability to video monitor their home at all times and have access to humidity, temperature, and air quality readings from their smartphones. In turn, State Farm will offer up to a 15% insurance discount for using the system (Yerak, 2015).

USAA is also taking advantage of the IoT connected home, but in a different way. USAA developed a patented data recorder that "uses sensors to detect temperature, wind speed, humidity, rainfall, vibrations, water pressure and electrical system voltages" (Yerak, 2015). They will use the collected data to find trends and adjust premiums to reflect the risk associated with the trends. They will also look to alert customers of possible problems or impending weather related issues. For instance, if there are particularly high winds, they may remind policyholders to reinforce their windows. The USAA is trying to employ as much Smart Home technology into their insureds' homes as they can because many of their policyholders are active military members who are deployed and may not have immediate access to their homes (Yerak, 2015). If USAA can accurately monitor dangers to the homes, the potential for loss is lower when the homeowners are away. The connected home market within the IoT is a growing venture for insurers and, if executed correctly, will be responsible for significant growth in the deployment of smart home products. It is projected that by the end of "2016, the global connected market is expected to reach $235 Billion" (De Armond, Lalancette, & Mulhall, 2015).
To be successful, insurers must be able to provide their customers value in Smart Home appliances. The problem manufacturing companies have been having is convincing the consumer that, for instance, the enhanced features of a smart home thermostat justifies the additional cost. By offering discounts and adding value, like smoke detector battery change reminders, insurers can exhibit to policyholders the importance of having a Smart Home.

The connected car, self, and home are helping insurers to educate their customers, lower their risks, and more accurately set premiums. Soon we will see drones flying over disaster zones to assess the property damage and devices that can use IoT to gather analytics and predict major weather events. Through investments in companies that have a vision for the future of the IoT, insurers can keep current with the trends and encourage their policyholders to do the same. However, with all of the connectivity comes a larger liability that presents a threat to consumers and insurers alike - cyber risk.

A constant stream of data is flowing through the IoT, whether it be tracking where the location of a car or the temperature of a home. The massive amounts of data create more privileges for hackers to access the data and use it to harm the consumer or the item. Although cyber insurance has been on the market for a few years, it has previously been used to cover loss of personal information. With the IoT, the consequences could be much more detrimental. In a controlled experiment, hackers have demonstrated the ability to hack into Jeep's onboard computers and take control of a car or, potentially, all models within a given geographic area. Insurers are unsure how to insure a loss of that magnitude (Mullaney, 2016). As insurers invest in new IoT products, they may consider if the product is properly protected against a cyber attack.

August. Inc. failed to protect their consumers against cyber risk when they produced a smart lock with the ability to unlock your door from a smartphone application. Bluetooth connectivity allows the homeowners to unlock their door remotely, without a physical presence. Unfortunately, two major flaws created a significant cyber liability. First, anyone who had the

August smart lock app had access to the names of the Bluetooth enabled locks in their vicinity. Hackers could easily locate locks and determine the location based on the name. The second security issue was the app allowed intruders to unlock the door by sending a command to the server. Furthermore, August Inc. created a firewall to block against this problem, but there is no way to update the device to obtain the firewall (A. Haas, M. Haas, & Weinert, 2015, 2.3.1). Many consumers are looking for products to make their daily lives easier, such as keyless entry. However, the benefits it brings to daily life is proving to come with unintended costs to the insured and insurer.

Currently, "if a device connects to the internet- it's vulnerable" (Gerking & Smith, 2015). This will change, especially as insurers are able to gather information on where the risks lie and what the hackers are capable of. Insurers will need to try to gain information on a theoretical basis, rather than waiting for losses to occur. The challenge is staying ahead of the hacker community. The ever increasing connectivity of the world is presents the potential for a catastrophic loss. Lloyds of London hypothesized if a hacker were to take over the electric grid of the Eastern United States, losses could be as high as $2 trillion with only a quarter covered by insurance (Gerking & Smith, 2015). Although a cyberattack was the peril, the losses may cross over multiple traditional lines of insurance ranging from business interruption to property damage.

Cyber risk is presenting a huge obstacle for companies, consumers, and insurers. With the rate technology is developing, it is unlikely that cyber risk will subside anytime soon. Consumers trust insurers to solve their problems and therefore, insurers need to stay in front of the risks. To protect their policyholders and themselves from the losses associated with cyber attacks, insurers must write clear cyber policies and renewals; promote protection by partnering with tech companies focused on cyber security and leading edge safety products; and adapt underwriting to evolving risks while providing discounts for early adopters of safety programs and products.

Consider a cyber attack on an energy supplier where a hacker causes gas to be released igniting a fire (Nicholson, 2014). Not only have the company's systems been breached, but there is property damage, injured employees, business interruption, and reputation damage. Through "the interconnected nature of networks…exposures multiply significantly" (Artemis, 2015). Insurers need to consider this trickle down effect when writing their cyber risk policies and renewals, what exactly should cyber insurance cover? Previously when cyber insurance was written, it only covered loss of personal data to hackers (Mullaney, 2016). As the Internet of Things has increased the amount of data that is accessible to consumers and to hackers, the cyber risks have grown more malicious. It is no longer only about individual identity theft. A hacker could take over a car or an entire store's credit card storage data base. We need insurance policies that can cover attacks of this scale, but insurers and policyholders need to know exactly what is covered. Travelers is one company that offers some comprehensive cyber coverage. They offer coverage of regulatory defense expenses, network and information security liability, communications and media liability, e-commerce extortion, funds transfer fraud, business interruption and additional expenses, crisis management expenses and computer restoration expenses (Travelers, 2015). Traveler's cyber insurance provides comprehensive coverage for lower cyber risk industries, such as smaller firms that do not rely on the internet for all of their data. They offer a variety of technology and liability coverage, but not much protection for human and intellectual capital. Marsh offers coverage that would appeal to consumers in industries with high chances of cyber attack. Their coverage encompasses operational disruption, regulatory compliance, lawsuits and reputational harm, and employee exposures (Marsh, 2015). Both companies have succeeded in writing clear policies that provide greater protection to policyholders. The next step is ensuring the policyholder is taking steps to protect themselves.

Insurance should be an addition to, not a substitute for, proactive cyber security. However, consumers may rely on the insurer if they know they are covered, rather than making all the necessary financial investments to stay current with the ever changing threats. Insurers can mitigate this risk in a number of ways. We have already seen how insurers are using the IoT to encourage healthy, safe behaviors from their customers in their cars, work lives, and homes, why not implement that same principle here? Partnering with cyber security tech firms to offer rewards and discounts to their policyholders who implement protective technology into their networks would be a great way to encourage security and lower the insurers risk of facing a claim.

Before an insurer faces a claim, they want to make certain policyholders are paying fair premiums based on their overall risk profile. Underwriting cyber risk is difficult because of the nature of the risk and the small loss history. Tech start up companies seized this opportunity to create benchmarking or rating systems to score companies based on their cyber risks. Insurers will be able to use this rating to price premiums and decide what coverage to offer a company. The company could use this rating to decide how much cyber coverage they should get. Do they need all of the features Marsh offers or are Traveler's features enough? CRC Insurance Services is working with UpGuard's rating system CSTAR, to "assess risk for both insurance providers and businesses" (CBInsights, 2016). QuadMetrics, created from researchers at the University of Michigan, features a prediction index for future security breaches and has partnered with the Department of Homeland Security (CBInsights, 2016). The score presents a way for insurers to have a better idea of their potential losses without the need for extensive loss history. Insurers do have options when it comes to protecting themselves against the threats of cyber risk the Internet of Things has brought about, but they must be proactive in controlling the risk before it occurs.

Cyber risk presents an unfamiliar challenge to individuals, companies, and insurers. While the exposures associated with the potential attacks are costly and ambiguous, the opportunities the IoT have provided are extraordinarily beneficial and outweigh the exposures. Today we have the ability to underwrite policies based on real time data we receive as policy holders drive. In a few years, the IoT will put self-driving cars on the market. The possibilities are endless and insurers are in the forefront of the innovation. As the IoT expands into all facets of everyday life, insurers need to continue to develop partnerships and push for more regulation and security on the connected devices. Through the eagerness of solution driven, innovative insurer and IoT startups, cyber risk will be manageable, our connectivity will grow as a result. Carpets that alert of intruders, drones that survey property damage; what will be next in the Internet of Things?