



FALL 2018
White Paper Contest Winners

Bryan Sanders

University of Houston-Downtown

Autonomous Vehicles

Maya Stefanovic

Arizona State University

Autonomous Vehicles

Brendan Sturm

Arizona State University

Cyber Security

**Autonomous Vehicles:
Navigating Through the Technology
(A Claims and Risk Management Perspective)**

by

**Bryan Sanders
University of Houston – Downtown
November 30, 2018**



Executive Summary

Autonomous vehicles are an exciting emerging technology which were once considered science fiction, but is now a definitive reality, even as of today. While driverless technology is continuing to improve and evolve, society has yet to witness the mass production of fully autonomous vehicles. It is clear our world is destined for this future. The intent and scope of this research is to examine autonomous vehicle technology from the perspective of a claims adjuster or a risk management professional. This includes a review of the technology surrounding autonomous vehicles, the implications of this technology within the claims environment, and an examination of the most significant opportunities and threats associated with the emerging autonomous vehicle industry.

The importance of this research will help to educate and guide our Wholesale & Specialty Insurance Association (WSIA) professional members on challenges this technology may bring in their careers as claim and risk management professionals. Online publications and articles from various sources ranging from business, government, and collegiate education were utilized as the primary research method employed for this paper. The conclusions opined is centered upon the importance of understanding the impact of this technology in the context of administration of automobile insurance claims. It is imperative for claims adjusters to investigate all the facts to properly assess liability when accidents involve autonomous vehicles. In addition, careful examination of policy contract provisions is crucial to determining whether appropriate coverage or if additional coverages may apply to a loss such as from products or software liability policies. While fully autonomous vehicles and the resulting transportation infrastructure is predicted to significantly reduce automobile loss frequency, the complexity of losses arising from such accidents can be significant. A tremendous opportunity exists for insurance organizations to

benefit from the rising industry of automated passenger transportation services by developing new insurance products, but they must proactively engage within the industry to be successful. This engagement would include understanding the threats that come with this technology such as insurance related legal and regulatory changes, managing complex liability losses, and understanding the importance of data analysis in helping to combat insurance fraud.

Based on my research I advocate the following insurance industry-wide changes in order for the organizations to maintain a competitive advantage in the market. Insurance companies need to re-examine policy contract provisions to effectively manage the future impact autonomous vehicles will have on coverage and liability. In coordination, risk management professionals must be able to identify and interpret these policy changes accurately. Claim organizations also need to modify the claim process because of autonomous technology to emphasize investigations into comparative negligence or identify subrogation potential from other sources of insurance products which will soon flood the market. Lastly, by sharing education and informational services such as those offered by WSIA when the time comes where our roadways are lined bumper to bumper with autonomous vehicles, claim adjusters and risk management professionals will be prepared to meet the challenges presented from such a dynamic technology.

Introduction

In 1908 when Henry Ford's model T first came off the factory production lines and onto the streets of America no one could imagine the impact his product would have on the American landscape. The mass production of an affordable mode of transportation distinct from any other at the time not only helped to spark economic growth, but also led to an incredible new product for property and liability casualty insurers. It must have been an exciting time to be in the

insurance business. Even more exciting is we have entered a similar moment in time with the introduction of autonomous vehicles. These new technologically driven vehicles have already begun making an impact on helping American roadways become safer, but are soon gearing up to make a more considerable impact on society and the insurance industry. There are many unanswered questions as to the effect autonomous vehicles will have on insurance; particularly regarding coverage concerns and liability risks. A prominent question would be determining who is liable for an accident when an autonomous vehicle is involved; is it the owner, operator, manufacturer, or software developer? Another question is determining where primary and secondary coverage exists and should contracts be modified accordingly? This research paper will dive into this wave of new and emerging technology in order to analyze the future impact on automobile insurance claims. The goal is to help inform and educate risk management professionals so they are fully prepared to meet the challenges which can be presented when investigating coverage and liability arising from the operation of autonomous vehicles.

History & Future

It is important to begin with an understanding of the brief history, current state, and future of this technology because “the arrival of autonomous vehicles is poised to dynamically transform the automobile industry and usher a new era of mobility.” (Chaturvedi, 2018) Accordingly, we should understand how the technology has altered the responsibilities associated with the maintenance and operation of personal passenger vehicles along with understanding what changes can be expected in the future. Autonomous vehicles are developed using driverless vehicle technologies. The primary technology by which autonomous vehicles operate is by using cameras. A 3D image can be created using four to six cameras that undergo image stitching, which is the process by which the surrounding environment can then be

visualized. To ensure a clear image is created, cameras with a very high dynamic range are



necessary. The photograph to the left (Lee, 2018) provides a depiction of this technology as found in this Tesla prototype. The additional technologies needed to develop driverless vehicles are global

positioning system (GPS), radar, lidar, and corresponding software. The advances in these areas of technology have made it economically viable for auto manufacturers to increase the use of these systems in many private passenger vehicles while having a level of accuracy up to 15 meters.

There are 5 phases that have been used to describe the level of driverless technology utilized in autonomous vehicles and can help us understand the current state of this emerging technology. Phase 1 involves vehicles which are essentially driver controlled but aided with automated driver assisting technology. Examples of common types of driver assistance provided include sensors which help with collision avoidance, lane departure assist, and parking assistance. In Phase 2, the autonomous capabilities include the ability of the vehicle to drive itself on major roads while returning control to the driver only on secondary streets. Cadillac has developed “super cruise” which entails full speed range adaptive cruise control and lane centering using sensors that automatically steer and brake during highway driving. In Phase 3, autonomous vehicles are developed with the ability for optional vehicle autonomy by allowing drivers to input a desired destination where the car would then automatically navigate through both major and secondary roadways. Tesla’s Autopilot is currently in development and is setting the standard for Phase 3 vehicle autonomy. Another Phase 3 autonomous vehicle comes

from Alphabet Incorporated who developed the WAYMO self-driving vehicle that is currently being tested in Arizona.

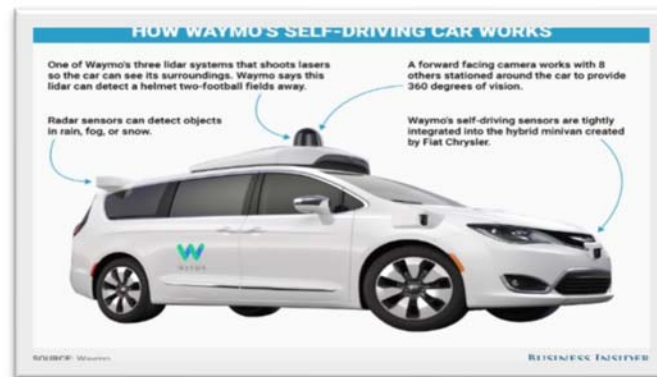


Figure 1: Waymo self-driving car (Lee, 2018)

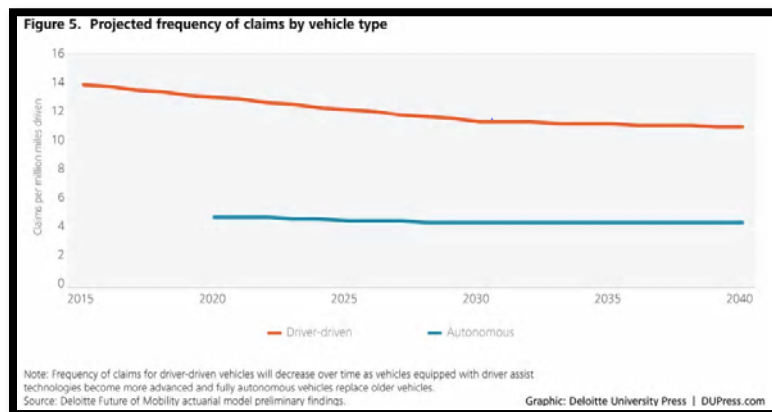
Phase 4 involves creating the infrastructure needed to assist with vehicle autonomy. Vehicles will have the ability to operate on a fully autonomous basis. Autonomous technology can outperform a human driver; however, infrastructure technology is needed to assist the vehicle to account for the effects from roadway construction.

In the near future, society will see the presence of fully automated vehicles as we enter Phase 5 of driverless technology. At that point vehicles will have all the necessary technology to operate without a driver and all roads will be equipped with the necessary technology to support autonomous vehicle operations. According to a research study completed by Intel “the mainstreaming of autonomous vehicles by 2050 provides an impetus to what Intel called the “Passenger Economy” driven by autonomous vehicles which would be worth \$7 trillion by 2050.” (Chaturvedi, 2018) Also, Accenture and Stevens Institute of Technology predict there will be as many as 23 million fully autonomous vehicles by 2035. We are clearly entering an exciting time where innovation and imagination is creating new products and services which will need appropriate insurance coverage to protect both businesses and consumers. If insurance

organizations are going to successfully manage the impact of driverless vehicles, it is important to address the implications this technology presents.

Implications

The implications of autonomous vehicles on the insurance industry and society are significant and should be fully explored. The scope of this paper will be refined to implications associated with insurance claims for which claim adjusters should be prepared to encounter. In much of the research many experts predict autonomous vehicles will help to provide safer cars and roadways and as a result insurance companies should witness reductions in loss frequency. The data so far does support this conclusion based on the projections noted in the graph below (Matley, Gandhi, Yoo, Jarmuz, Peterson, 2018).



This may seem to be a blessing for an automobile property and casualty claim adjuster's case load; however, advancements in the technology are still needed before the total benefits are

realized. It is true that driverless technologies have helped reduce loss frequency in many minor accidents such as how rear facing cameras and warning systems have helped to reduce parking lot accidents. However, claim adjusters and risk management professionals should be aware that even with such technology in place, thorough investigations are still needed to properly assess where liability for an accident may lie.

This leads to a significant implication for claim adjusters on how to properly assess liability in accidents involving autonomous vehicles. The importance of this implication is

evident by recent accidents involving autonomous vehicles where fatalities occurred. The first reported accident involving an autonomously driven vehicle occurred on May 7, 2016 and involved Tesla's Model S. The driver of the Model S was fatally injured when his vehicle collided broadside with a semi-truck crossing the highway in Williston, FL. At the time, the vehicle was traveling 74 mph and in autopilot mode which can control the car during highway driving. The car's sensor system allegedly failed to distinguish the large white side of the semi-trailer. Neither the autopilot nor the driver hit the brakes. Tesla Motors investigation reported to have found no defects in the autopilot camera system. Michelle Heron, a senior associate with Bristows LLP, helped to report the results of the National Highway Traffic Safety Administration (NHTSA) who concluded "that the camera failed to recognize the white truck against a bright sky but essentially found that the driver was not paying attention to the road way." (Herron, 2018) In addition, the NHTSA concluded that although Tesla's autonomous vehicle's system did not help to prevent the accident, it did perform as designed. The facts from this accident shows how critically important it will be for claim investigators to secure all relevant evidence as well as understanding the technology around autonomous vehicles and its potential impact when assessing liability. More importantly insurance companies should proactively work to amend policy contracts to effectively address the implication autonomous technology will pose on liability for a loss. For example, automobile insurance carriers can consider making policy contract changes under Section I – Liability Coverage to exclude damages caused as result of product failure in autonomous vehicle technology.

The second fatal accident involving an autonomous vehicle occurred on March 18, 2018. This accident involved a pedestrian who was fatally injured after she was struck by a Volvo autonomous Uber car. The pedestrian was crossing an uncongested road in Arizona around 10

pm. There seemed to be no indication that the driverless vehicle, which was in auto mode but with a safety operator on board, had attempted to brake or swerve to avoid the pedestrian. The facts of this case would warrant an extensive claim investigation and arguments can be made of comparative negligence; however, Uber reportedly reached a quick settlement agreement with the family. It has been reported that Volvo's CEO, Hakan Samuelsson said, "Volvo will accept full liability whenever one of its cars are in autonomous mode," (Huckstep, 2018) which may explain Uber's quick settlement. This accident provides claim professionals with an example of how important it is to also investigate all potential applicable coverage that may apply with the existence of autonomous technology. This includes insurance policies that cover a driver such as under a personal auto policy, or a commercial policy which covers automobile manufacturers, and even a product liability policy which protects companies who have developed driverless technology. Autonomous vehicles can open many additional risk exposures for all engaged in this industry and as such has quite an impact on the claims environment. Accordingly, I recommend claim organizations modify claim processes to place focus on examining the coverage implications associated with autonomous vehicles.

Another implication of autonomous vehicle technology is the rising cost and sophistication of repairs that are needed. This is important for claim adjusters to understand due to the impact this may have when processing claims. Risk management professionals also need to be cognizant of this fact when assessing an organization's loss exposures. Property damage loss costs have risen dramatically in the past decade which primarily appear to be driven by increased cost to repair technical components along with additional labor costs associated with using qualified and certified technicians to perform such repairs. According to an interview with David Williamson from AXA UK about the rising insurance costs, David comments "the fact is

that motor repair costs in the UK have gone up by 32% in the last three years. This is largely due to the costs from extra technology fitted in cars, much of it safety equipment.” (Huckstep, 2018) This can impact a claim investigation by determining whether a policy holder carries sufficient liability limits to cover the damages caused to a third party who was operating a vehicle with expensive driverless technology. Understanding the implications autonomous vehicles have on the insurance industry; particularly within the claims and risk management environment will also help lead to identifying opportunities and threats associated with this emerging technology.

Opportunities

There are many opportunities associated with the mass production of autonomous vehicles and the implementation of a passenger driven economic force. The passenger service industry has seemed to have evolved from commercial taxis, to personal business Uber drivers, and now to Google’s Waymo who is introducing driverless passenger services. As a result, insurance policies have also evolved to provide affordable and specific coverage protection in the event of a loss. New forms of insurance policies are needed for autonomous vehicles. An example of this new type of insurance policy can be seen from Adrian Flux’s Driverless Car Policy. This specialized policy contains specific language which dictates what circumstances may exist that would exclude coverage. Claim adjusters must be knowledgeable of changes in policy language or provisions to ensure the correct coverage is applied, determining if any exclusions would exist, and ascertaining subrogation potential against a liable third party such as from a commercial or products liability entity.

Another opportunity that has arisen from the emergence of driverless technology is the reduction in loss frequency. This trend is continued to be expected in the future as more and more vehicles are equipped with driver assisted technologies. Not only is travel predicted to be

safer but also the data now available from the safety features associated with autonomous vehicles can also be quite helpful for claims adjusters when disputes in the facts of the loss need further investigation. This situation enforces the need for insurance claim organizations across the globe to be fully prepared for the mass implementation of autonomous vehicles on our roadways. Chart 1 below shows which countries are most prepared for this emerging technology. I recommend insurance companies prepare claim and risk management professionals for emerging autonomous technologies by implementing continuing education courses for all claim and risk management professionals.

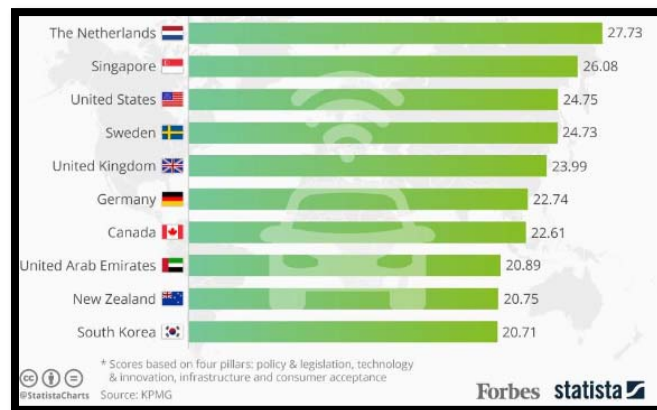


Chart 1: Countries prepared for Autonomous Vehicles (McCarthy, 2018)

An additional opportunity autonomous vehicle technology can provide claims professionals is with the use of data collection in helping to reduce insurance fraud. It is reported that “every incremental 10 percent reduction in fraudulent claims could result in industrywide savings of up to \$800 million.” (Matley, Gandhi, Yoo, Jarmuz, Peterson, 2018) The data driven foundation of many of the telematics and sensors found within safety features on autonomous vehicles can provide claim examiners with an effective tool against policyholders who choose to fabricate facts to fraudulently benefit when making a claim. The vehicle data has another advantage when it can also show when liability may rest on the manufacturer as opposed to a

driver with respect to a loss. Dr. Peter Diamandis, Executive Founder of Singularity University, points out “car insurance premiums are currently calculated according to the driver and traits of the car. But as more autonomous vehicles take to the roads, not only does liability shift to manufacturers and software engineers, but the risk of collision falls dramatically.” (Diamandis, 2018) Claim adjusters and risk management professionals will need to become experts in big data analytics.

Threats

As there are opportunities for an insurance claim organization associated with the mass implementation of fully autonomous vehicles into society, there are also significant threats. The most prominent threat is the unknown and ever changing legal or regulatory requirements. Insurance contracts are heavily regulated and because most are contracts of adhesion, a claims adjuster must be familiar with changes in the legal environment to ensure claims are handled in good faith. In addition, claim adjusters who investigate claims in multiple states are threatened as insurance regulations can vary between each state. In fact, the Insurance Journal reports “as of year-end 2017, state legislatures had done little to revise existing auto insurance laws for the potential insurance implications of autonomous vehicles. Uneven state legislative and regulatory progress may hinder insurers in designing and maintaining insurance programs that address autonomous vehicles.” (Perfetto and Blancher, 2018) This can pose challenges for insurance professionals who must interpret current policy language which may differ from changing insurance regulations regarding autonomous vehicles. This environment demands claims professionals to stay current on legal and regulatory matters within the jurisdictions for which they work.

Another threat associated with the implementation of driverless technology, whether partial or fully automated vehicles, is the complexity and cost associated with defending law suits especially where arguments of comparative negligence can be applied. We must prepare for the future where autonomous automobile accident investigations will not be conducted by federal organizations such as the NHTSA but rather local law enforcement and liability insurance claim adjusters. The complexity and always changing technology and the availability of supporting credible evidence can make investigations challenging. The potential for numerous co-defendants such as from manufacturers, technical product developers, or automobile services providers can add to the complexity of a lawsuit. The experts needed to testify can be costly and there are various other defense costs which can be surmounting to insurance companies or self-insured organizations.

Claim or risk management professionals should also be aware of the existence of new forms of data threat to organizations, such as Waymo, who will manage fleets of autonomous vehicles and looking to bring self-driving cars to the masses. Such organizations will need help from risk management professionals with identifying risk exposures and analyzing policy contracts to ensure proper coverage exists. However, more importantly “from an insurance perspective, both fleet operations and leasing companies are at risk of their vehicles being victim to data breaches and cyber-attacks and as such, there will almost certainly be heightened levels of data security as more autonomous fleets begin to be rolled out.” (Brooks, 2018) Therefore claim adjusters should be aware of this threat when investigating autonomous vehicle claims. While these threats may not be prevalent today, it is imperative claim and risk management professionals prepare for all the future threats and opportunities which will arise from such a remarkable emerging technology and which may arrive much sooner than expected.

Works Cited

- Brooks, M. (2018, October 1). How Will We Be Insuring the Fleets of the Future? Retrieved from <https://realbusiness.co.uk/fleet-insurance/>
- Chaturvedi, A. (2018, October 25). Intel Study: People Certain About Self-Driving Cars Hitting Roads by 2050. Retrieved from <https://www.geospatialworld.net/blogs/intel-self-driving-cars-roads-by-2050/>
- Diamandis, P. (2018, October 18). Will Tech Make Insurance Obsolete in the Future? Retrieved from <https://singularityhub.com/2018/10/18/will-tech-make-insurance-obsolete-in-the-future/#sm.00001a2e35f5drcy9zphkm53hseb8>
- Herron, M. (2018, October 9). Who's Going To Drive You Home? Liability for Autonomous Vehicles: Part 1. Retrieved from <https://www.lexology.com/library/detail.aspx?g=440704f4-e775-40c2-a617-e175c9e5bbb4>
- Huckstep, R. (2018, September 3). Four Ways Autonomous Vehicles Will Change Auto Insurance. Retrieved from <https://www.the-digital-insurer.com/blog/insurtech-impact-autonomous-vehicles-auto-insurance/>
- Lee, T. (2018, October 24). Ford's Plan for Driverless Cars Goes Beyond Technology. Retrieved from <https://arstechnica.com/cars/2018/10/ford-to-test-driverless-cars-in-washington-dc-ahead-of-2021-launch/>
- Matley, J., and M. Gandhi, E. Yoo, B. Jarmuz, S. Peterson (2016, May 13). Insuring the Future of Mobility. Retrieved from <https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/mobility-ecosystem-future-of-auto-insurance.html>
- McCarthy, N. (2018, October 23). The Countries Best Prepared for Autonomous Vehicles Retrieved from <https://www.forbes.com/sites/niallmccarthy/2018/10/23/the-countries-best-prepared-for-autonomous-vehicles-infographic/#745312bf3df2>
- Perfetto, S. and A. Blancher. (2018, May 17). The Road Ahead for Autonomous Cars and Auto Insurance. Retrieved from <https://www.insurancejournal.com/news/national/2018/05/17/489282.htm>

THE FUTURE OF STREAMING TRANSPORTATION SERVICES

Maja Stefanovic
Arizona State University
November 25, 2018
Dr. Jelena Milovanovic ACIA, AIAA, Ph.D.

INTRODUCTION

Imagine a world where all the cars on the road are navigating without a human driver. Headlines involving autonomous vehicles that do not require drivers are ubiquitous, but what about when cars don't require owners? Autonomous vehicles are likely to revolutionize our transportation system and cause a large shift from an ownership model to cars on demand.

Uber and Lyft have replaced hailing a taxi with the simplicity of ordering a ride using a smartphone, while those who do not own cars may turn to Zipcar for its on-demand car use. The combination of Uber, Zipcar, and the potential of autonomous vehicles creates ownerless stream driving. Stream driving is a concept that when an individual requires a ride, a car is sent, takes the individual to their destination, and then departs. In the stream driving transportation model there will no longer be a need for vehicle ownership. This is not a relatively new concept; ten years ago music was purchased on CDs while now it is streamed on apps such as Pandora and Spotify.

Currently, auto insurers use a variety of rating variables to predict future losses. The purpose of variables, like the policyholder's gender, age, driving record, and accident frequency, is to help insurers create an accurate assessment of the risk they are absorbing in order to price premiums adequately. As society shifts to a streaming transportation model, assessing the risk associated with insuring autonomous vehicles and pricing premiums will become more complex. The specific challenges come from the lack of data and limited margin for error when pricing premiums. While the shift to a

streaming transportation model could affect many traditional industries, such as auto manufacturers and insurers, stream driving could create new opportunities for non-admitted carriers, such as cybersecurity, product liability, public infrastructure, and goods-in-transit insurance.

THREATS ASSOCIATED WITH AUTONOMOUS VEHICLES

Two major considerations should be taken into account by non-admitted carriers insuring fleets of autonomous vehicles:

- Data analytics regarding autonomous vehicles
- Limited room for error

DATA ANALYTICS

As society begins to shift into the onset of driverless vehicles, initially sparse data will provide challenges to developing accurate insurance rating models. Insurance companies have always relied on data to assess risk, set premiums, and to win and retain customers (Silicone Valley Data Science). However, the lack of data related to autonomous vehicles might result in inadequately priced premiums by the non-admitted carriers.

On the other hand, once data does become available, transmitting and storing such data might pose additional issues. As autonomous vehicles become more connected between each other, infrastructure, and other sources, data will grow exponentially (McKinsey&Company). In this highly interconnected environment, cars will

constantly be on the road generating real-time and comprehensive data. Expects from the KPMG Automotive Team believe that the ability to gather, aggregate, and harness the information will be critical (KPMG). However, the actual capability to gather and manage such a large wave of data will be strenuous.

NO MARGIN FOR ERROR

Considering that carriers currently insuring standard automobile insurance have been at a break-even point for the past several years, there will be a limited profitability cushion for non-admitted carriers to erode in the driverless vehicles line of business (KPMG). Figure 1 below shows that the personal lines aggregate combined ratio has been steadily increasing for the past 10 years. Personal auto insurance is specifically responsible for these consecutive underwriting losses due to inadequate pricing and adverse claims trend (Property Casualty 360). Simply put, profit margins have been shrinking in the personal auto industry. Since insurers are having difficulty generating a profit in a normal market - one without fully autonomous vehicles, writing new business involving driverless cars without this profitability cushion could pose a risk.

Personal Lines Aggregate Underwriting Performance

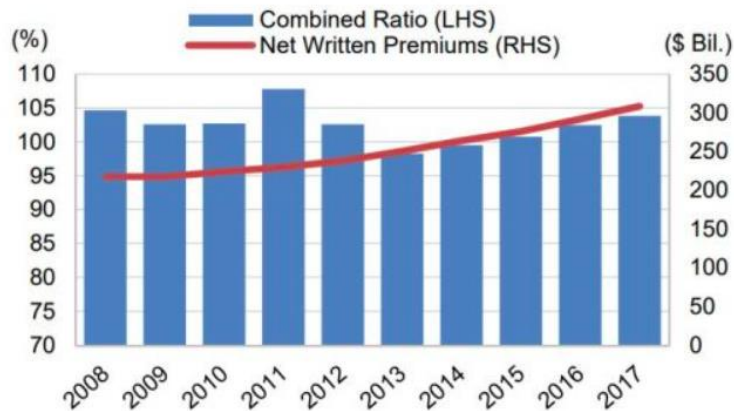


Figure 1: Personal Lines Aggregate Underwriting Performance. Image from Property Casualty 360.

INDUSTRIES IMPACTED

AUTO MANUFACTURERS

On-demand autonomous vehicles will slowly switch society from an ownership model to a streaming transportation model. However, will these ownerless self-driving vehicles push traditional vehicle manufacturers and suppliers, like Ford, Toyota, and many others out of business? The answer to this question depends solely on how each manufacturer reacts. McKinsey & Company identified four strategic stances car manufactures can take on. Automotive players will either introduce increased levels of advanced driver-assistance systems (ADAS) in their vehicles, focus specifically on the “accessible mobility” consumer segment, invest in autonomous vehicles research, or avoid entering the autonomous vehicle market (McKinsey & Company).

Even though the automated vehicle revolution will push society away from an ownership model, the demand for cars will still exist. Figure 2 below shows that ownerless vehicles will, in fact, grow vehicle sales by an estimated 2% annual rate. The annual rate of growth proposes that automotive revenue will rise by approximately 1.5 trillion dollars between 2015 and 2030 (McKinsey & Company). With the combination of shared mobility and autonomous vehicles, the same car will constantly be on the road picking-up and dropping off passengers. Vehicles in constant motion will thus quickly increase annual mileage. Frequent replacement of aging autonomous vehicles will provide the existing manufacturers with the opportunity to grow their business as well as increase the possibility of new car manufacturers entering the market.

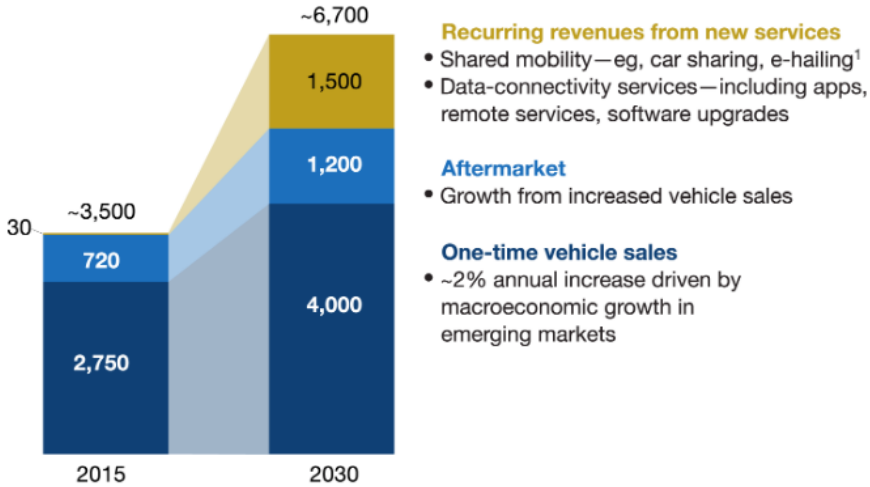


Figure 2: Automotive revenue pool (\$ billion). Image from McKinsey & Company.

AUTO INSURERS

Stream driving will greatly impact the insurance business and risk management, specifically the auto insurance industry. Safety is the paramount importance of autonomous vehicles since their development has the potential to eliminate human error while driving. According to vice president at Fortegra Financial Corporation, Scott McLaren, more than 3,000 people were killed and 431,000 injured by distracted driving in the United States in 2014 alone (McLaren). The contributing factors were human errors including fatigue, cell phone usage, aggressive driving, and running red lights. In a 2015 interview, Elon Musk, CEO of Tesla, pointed out that recent advances in autonomous vehicles could lead to human-operated vehicles to become illegal (McLaren). Musk's prediction comes from one simple reason: safety.

As vehicles begin to make decisions on their own, a shift from personal coverage to other forms of coverages will likely occur. With the vehicles using built-in software control algorithms to react to various driving scenarios, the potential liability for the software developer or car manufacturer will likely increase. For example, if an autonomous vehicle crashes into a building who is responsible? The current thought is that car manufacturers will be liable for accidents involving autonomous vehicles. The chief actuary of Insurance Information Institute, James Lynch, believes that if car manufacturers must bear the entire cost of insuring vehicles, that could create a long-term expense which could discourage manufacturers from technological development that will ultimately lead to safer roads (Noguchi). If autonomous technology should save lives but there is still potential for software glitches, and auto manufacturers will require

protection against the risks at stake. As a result, car manufacturers will turn to non-admitted carriers to cover the risks associated with manufacturing complex algorithm-controlled vehicles. The anticipated growth in the auto manufacturing industry due to autonomous vehicles, ensures car manufacturers will bring a plethora of opportunity for non-admitted carriers to write profitable liability coverage.

FOUR OPPORTUNITIES

Human error is not the only danger to vehicles, owners, and insurance companies. Like the risks associated with traditional vehicles, autonomous vehicles can still get stolen, damaged, or destroyed. Along with traditional risks, autonomous vehicles also bring in new risks and growth opportunities for non-admitted carriers- specifically, public infrastructure insurance, cybersecurity insurance, product liability insurance, and goods-in-transit insurance.

PUBLIC INFRASTRUCTURE INSURANCE

With autonomous vehicles comes an increased chance of catastrophic accidents. For driverless vehicles to operate, they will rely on being connected to a cloud server system (or grid). In vehicle-to-infrastructure control (V2I), the infrastructure helps coordinate vehicles by gathering global and local information on traffic and road conditions to impose certain behaviors on a group of vehicles (Glielmo). For example, the velocity, acceleration, and inter-vehicle distances are suggested by the infrastructure based on traffic conditions via wireless connections. Vehicle-to-infrastructure control brings additional risk to the table. Communication problems in the

system can potentially cause catastrophic damages if the satellite network which guides the navigation of driverless cars were to fail or is hacked. Once again, non-admitted carriers have the potential to grow business volume by offering coverage against network communication problems.

CYBER SECURITY INSURANCE

Autonomous vehicles bring significant new risks; such as breaches of cybersecurity. The potential of a criminal hacking into the vehicle's connected cloud server to cause injury or the vehicles computer system to gain information presents significant data security risks. If a banks software system is hacked, money can be lost; in the automotive industry, it is real lives that are at risk (Milliman). Of course, these exposures exist today, however, reinsurer Munich Re stated that the potential for cybersecurity threats will grow as vehicles become more connected to each other, the internet, and other networks (Munich Re).

The connectedness with the other vehicles on the road will give hackers different levels of access to damage if they breach the systems security barriers. Just recently, Charlie Miller, a security engineer at Twitter, and Chris Valasek, director of security intelligence at IOActive, plugged a MacBook into a car's computer to blast the horn, brake suddenly, cause sudden jerks in the steering wheel, spoof the GPS, and confuse the speedometer (Milliman). Miller and Valasek only had access to a single car's computer, but through autonomous vehicles, entire fleets of connected cars will be at risk.

Cybersecurity insurance is a vastly growing opportunity. According to a report from A.M. Best Co. Inc, a total of \$1.34 billion in premiums was written in 2016, a 34.7% increase from 2015. Cyber insurance is projected to grow from a \$7.5 billion to a \$20 billion business by 2020 (Insurance Journal). Non-admitted carriers can use this opportunity to actively offer coverage against the risks associated with cybersecurity breaches related to autonomous vehicles.

PRODUCT LIABILITY INSURANCE

Autonomous vehicles will shift the risk from human to technological error. The possibility of the software failing or the automated driving system not responding will almost certainly exist. With the autonomous system controlling the vehicle, liability will shift from the operator to the manufacturer. For example, a Tesla driver died while his car was in auto-pilot mode and drove into a turning tractor trailer (Milliman). The software in the Tesla vehicle had failed to react in time. In this case, the manufacturer was liable for the damages and bodily injuries. Accidents that cause property damage and bodily injuries are nothing new, the only difference will be the shift from car owners to car manufacturers purchasing the liability coverage.

Opportunities for non-admitted carriers to offer new liability coverage for autonomous-vehicle manufactures will rise. Since these vehicles will be extremely complex, with advanced sensors, connectivity, and software control algorithms, they will most likely be held to technical standards that may require maintenance on a regular

basis (Munich Re). As a result, car manufacturers will demand liability coverage for failure to maintain or adhere to self-driving protocols. In any case, it will be costly for manufacturers to defend themselves against lawsuits and many will choose to transfer their risks to non-admitted carriers.

GOODS-IN-TRANSIT INSURANCE

As the streaming transportation model eliminates the need for personal owners, some business will still have the need to own their own fleet of autonomous vehicles as a part of their business operations and thus need additional coverage for goods-in-transit. These businesses need goods-in-transit insurance which non-admitted carriers offer to protect their inventory from being lost, stolen, or damaged while in transit (ZAIL). By expanding the goods-in-transit insurance coverage to cover autonomous vehicles, non-admitted carriers can increase business growth.

SUMMARY

The development of autonomous vehicles and stream driving will be more than just a big change to the current transportation system. The new risks associated with autonomous vehicles will bring business growth opportunities to non-admitted carriers. As autonomous vehicles become standard, risk assessment will become more complex – involving how often the vehicles are hacked, the likelihood of the internal vehicle or cloud systems failing, as well as the usual risk of vehicles being lost, stolen or damaged while in transit. As a result, there will be a demand for public infrastructure, cybersecurity, product liability, and goods-in-transit insurance.

Non-admitted carriers who understand the data analytics behind stream driving and the limited margin for error when pricing premiums will be in the best position to capitalize on new opportunities. One method that non-admitted carriers may use to mitigate these challenges is through advances in data analytics. The ability to gather and manage real-time data generated by the autonomous vehicles will eventually result in more accurate pricing models. In any case, the streaming transportation model will ultimately require the current non-admitted carriers to drastically shift their business model in order to write profitable insurance coverages in the new stream transportation medium.

Works Cited

- Cyber Insurance Premium Volume Grew 35% to \$1.3 Billion in 2016. *Insurance Journal*, 23 June 2017.
- Data Opportunities in Insurance.” *Silicon Valley Data Science*, 19 Sept. 2017,
- Heft, Jayleen R. “P&C Personal Lines Results Worsen despite Auto Improvement: Fitch.” *PropertyCasualty360*, 14 June 2018.
- KPMG “Marketplace of Change: Automobile Insurance in the Era of Autonomous Vehicles.” *KPMG Insurance*, Oct. 2015.
- McLaren, Fortega Scott. “Autonomous cars could drive auto insurance to extinction.” *VentureBeat*, VentureBeat. N.p., nd. Web. 16 Oct. 2017.
- McKinsey & Company “Monetizing Car Data New Service Business Opportunities to Create New Customer Benefits.” *McKinsey & Company*, Sept. 2016.
- Milliman. “Connected cars and the cybersecurity risks of the future.” *Milliman*. N.p., nd. Web. 17 Oct. 2017.
- Munich Re. “Autonomous Vehicles.” *Munich Re*, 2016. Web. 17 Oct. 2017.
- Noguchi, Yuki. “Self-Driving Cars Raise Questions About Who Carries Insurance.” *NPR*, NPR, 3 Apr. 2017. Web. 20 Oct. 2017.
- Paul Gao, Hans-Werner Kaas, Detlev Mohr, and Dominik Wee. “Disruptive trends that will transform the auto industry.” *McKinsey & Company*. N.p., nd. Web. 16 Oct. 2017.
- Zurich. “Goods in Transit Insurance.” *Zurich Australian Insurance Limited*.

Cyber insurance in the Excess and Surplus Lines: A Modern-Day Gold Rush

Brendan Sturm

Senior

Arizona State University

Dr. Jelena Milovanovic, ACIA, AIAA

Introduction

Data is the new gold and insuring data is the new gold rush. Data protection methods aren't unbreakable; they merely act as a deterrent for hackers. For disruptive cyber attacks, businesses need cyber insurance to help indemnify the loss of business, reputation, and to provide services to those breached.

Pricing cyber risk is incredibly difficult due to small sample sizes, reporting bias, lack of insurance specific data, and a lack of an obvious exposure base. In the wholesale market, carriers are more willing to write reasonably high loss limits on cyber policies – even when there is lack of data. Making groundbreaking discoveries and gaining market share in this line of business will take a sizable risk appetite and creativity, making surplus lines the ideal area for innovation.

State of Cyber insurance

Cyber insurance exists to protect individuals and businesses against risks related to liabilities associated with breaches of privacy and information security. These policies cover investigation, business losses, notification, lawsuits, and even extortion related to data breaches. Cyber policies are mainly written as stand-alone product, allowing for more customization to fit the needs of the insured than possible with a cyber endorsement. Common coverages include: loss of business income, extortion, corporate data risk, property coverage, and costs relating to reporting cyber breaches including legal fees. Insurers are wary of the loss potential, as such “many insurers are also setting limits below the levels sought by their clients” and imposing “restrictive exclusions

and conditions”(O’Hearn 5). The combination of strict underwriting criteria and low policy limits is evidence that insurers are well aware of the unique risks associated with cyber coverage.

Currently, cyber insurance is a niche, but sharply growing line of business. A report from A.M. Best Co. Inc stated a total of “\$1.34 billion in premiums written in 2016, a 34.7% increase from 2015” and projects that the line will grow to be a 7.5 to 20 billion dollar line of business by 2020 (Insurance Journal). Of this premium, an estimated 90% is in the non-admitted market. (Greenwald)

Cyber breaches are incredibly costly in both financial terms and consumer trust. The average cost of a data breach is \$3.62 million according to the 2017 Ponemon Institute study (Ponemon Institute 1). When consumer information is stolen, companies are required by all 50 states to report the breach to consumers in writing (National Council for State Legislatures).

In addition to the costs of the notification, companies must:

- Pay legal fees to defend against class action lawsuits, if filed.
- Rebuild consumer trust, usually involving some sort of identity protection and credit monitoring service.
- Account for lost income as a result of any possible outages of their service.

For example, when Equifax had a data breach, they offered a credit and identity monitoring service in an attempt to control the damage, and restore some piece of their tarnished reputation.

Credit monitoring was available from the day the breach was announced, September 8, 2017, until January 31, 2018.

The cyber landscape is continuously evolving as more and more data is being shared on the cloud, shifting the duty to safeguard data from the user to the business. A data driven economy has made individual records much more valuable. As a result, new laws are being developed to more accurately define insured's duty to safeguard sensitive data, but with this comes the increased risk of loss contingencies.

Risks and Implications for the Non-Admitted market

Cyber risk is a low frequency high severity line, creating a significant demand for quality underwriting. According to a NetDiligence study, the median cyber claim payment was \$49K and the average claim payment was \$495K. It is important to recognize that breaches are not the only way to trigger a claim. Data breaches are by far the most expensive cyber claims with an average cost of \$3.62 million. However, there are additional risks companies face including simple recovery of lost data resulting from system glitches. Exposure to large losses can be dangerous, but it is important to understand which risks each individual insured faces to better determine how to underwrite the policy. Breaches have become more expensive over time. In figure 1 the steady increase in per capita costs of cyber breaches is shown.

Figure 1. The average per capita cost of data breach over the past 12 years
 Bracketed number defines the benchmark sample size

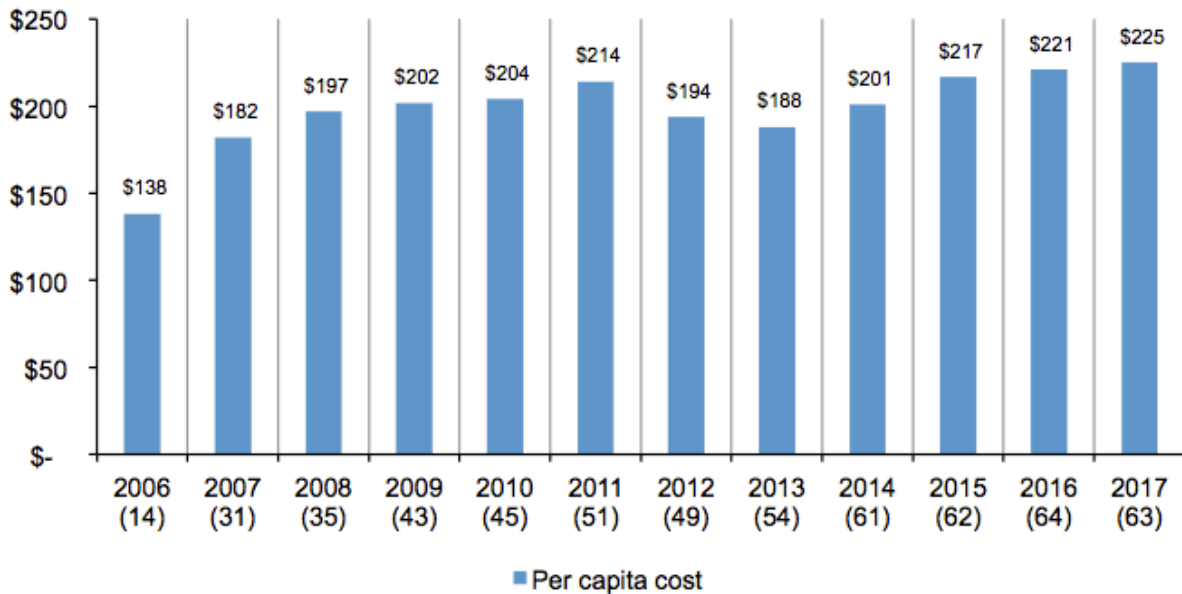


Fig 1. Data breach over time. Image from www.tripwire.com/state-of-security/security-data-protection/report-average-organizational-and-per-capita-costs-of-data-breach-reach-new-highs/.

Health and financial services breaches are the most expensive. Generally, the more personal the information, the higher its value. A person’s health history and finances are generally kept hidden, except to trusted professionals, which is why it is the most expensive record to insure.

Figure 2 details cost per record by industry.

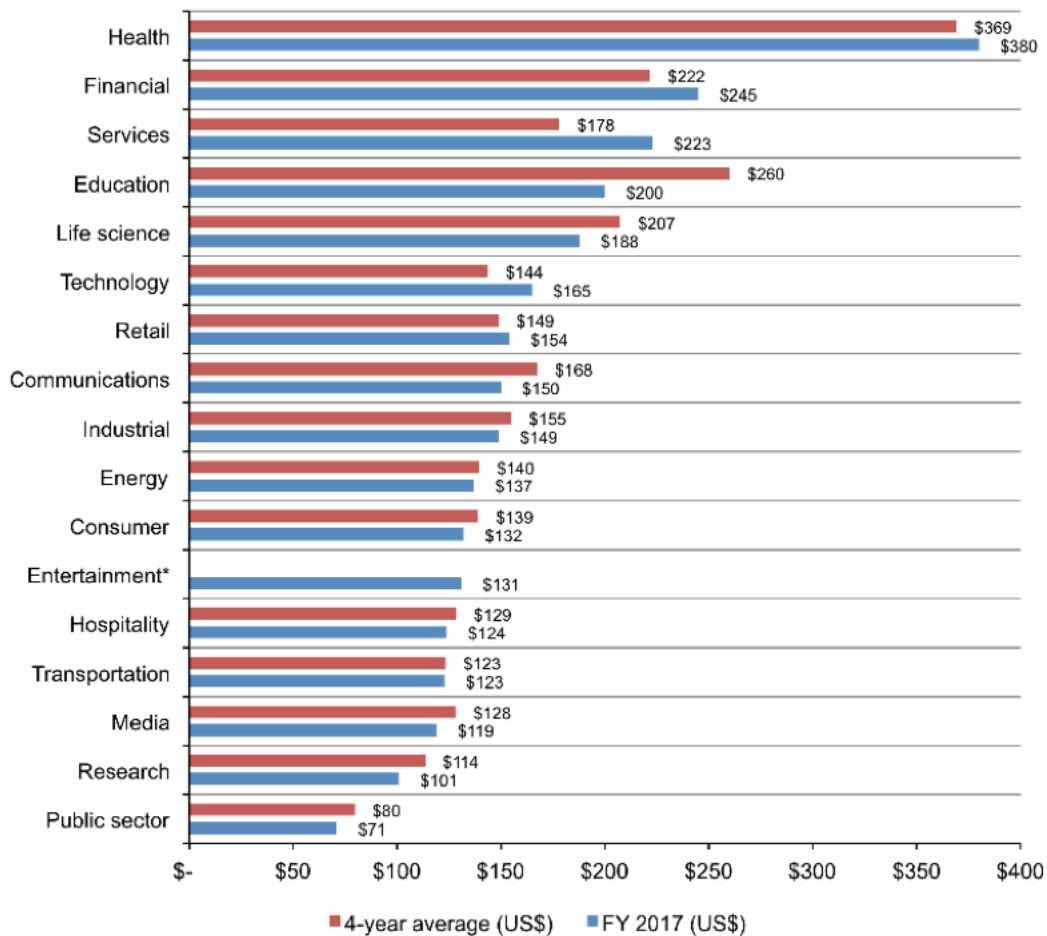


Fig.2. Cost per compromised record, by industry. Image from IBM and Ponemon Institute report 2017.

Moral hazard risk is high in cyber risk. As Figure 3 depicts below, insurers should beware of employee involvement in claims. NetDiligence’s study claims “insider involvement in 30% of the claims” and “staff mistakes (9%) and rogue employees (7%)” are common causes of loss (“2016 Cyber Claims Study” 15). Exclusions or strict policy language can be used to protect the insurer against losses due to internal mistakes or moral hazard, allowing the insurer to avoid some of the moral hazard present in the line.

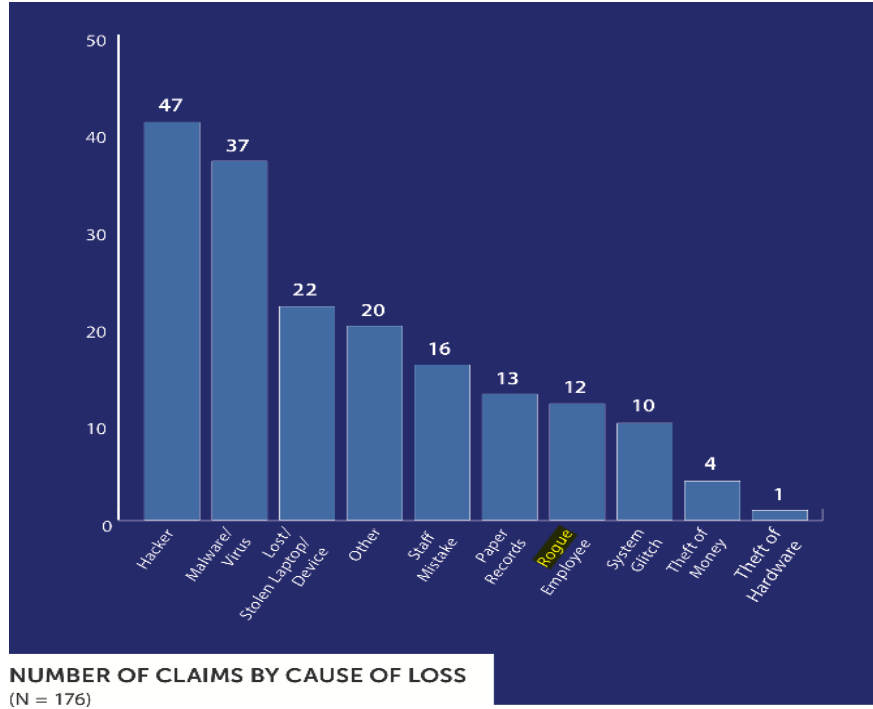


Fig. 3. Claims by cause of loss in 2016. Image from Netdiligence, compilation of data from many of the largest cyber insurers, including AIG, Travelers, XL Group, and Zurich NA

Independence is an important concept in insurable losses, but unlike many other lines of business, risks associated with cyber claims are rarely independent. A major vulnerability in one commonly used system could cause claims to start coming in from a plethora of firms using the flawed system. For example, in 2017 MacOS High Sierra had a bug which allowed anyone to access your computer by entering “root” as the username (CNet). Widespread data breaches could have been committed if hackers gained access to Macs with this issue, either remotely or in person. Homogeneous risks can be mitigated by incentivizing diversity in IT set-ups. Some companies, such as Wurzler Underwriting Managers offer clients premium credits if they use

Linux or Unix servers rather than Windows NT because these systems are less susceptible to attack (Kesan 28).

Opportunities for non-admitted markets

Customization

Innovation is possible in the non-admitted market because policies can be altered with minimal regulatory approval. Non-admitted markets allow for much more customized contracts and speed-to-market, giving the specialty carriers a significant advantage in adaptability within the ever-changing cyber landscape. Non-admitted carriers should take advantage of their ability to tailor contracts to customer needs, as this will allow for a wider spectrum of cyber products in the market place and increase availability. The insurers choice to tailor policy language to exclude specific vulnerabilities, in conjunction with the ability of large purchasers of insurance to negotiate their coverage, will allow both parties to reach an agreeable form of protection. Customized coverage could both be more cost-efficient for the insured, and potentially have more predictable, less frequent loss experience for the insurers.

Legislation

The current legislative climate is hastily adapting to the times. New York recently passed a law that requires businesses with at least \$5 million in revenue to “submit artifacts to support they have a cybersecurity plan of operations to include remote penetration testing, onsite vulnerability

assessments, and even demonstrate a CISO is in place” (Schoenberg). Potential widespread application of similar laws mandating higher levels of security would benefit the non-admitted market by increasing the premium volume and the size of the risk pool.

Recent laws regarding notification after data breaches have made breaches more expensive, and as a result data governance has become a large priority. Cyber insurance is a great way to complement a cybersecurity plan that is already in place. Insurers are taking a more active role in risk management with cyber lines. AIG, the largest writer of cyber policies, has strategic partnerships with IBM and cyber security companies to help their insured population to understand their risks and how to best limit them (AIG). This active step in limiting insured risk is similar to health insurers using activity monitors to incentivize active lifestyles. Non-admitted companies could become the ‘one stop shop’ for all things cybersecurity related by developing industry best practices and utilizing their relationship with the insured as a marketing opportunity.

Risk screening

Attracting technology experts, even ex-hackers, as specialty underwriting advisors will allow for a better understanding of the risks present in insured’s data protection systems. Financial firms have been utilizing the advice from cybersecurity experts for years in order to better protect their data, and it’s time for insurers to utilize the advice of these experts for pricing and risk screening.

Market share

Currently, American Insurance Group (AIG), Chubb, and XL Group command about 45% of the market for cyber insurance. (Insurance Journal). Figure 4 below shows the direct written premium by carrier for the cyber insurance market in 2016. Larger P&C insurers have yet to make a strong push into the cyber lines. The ideal time is now for non-admitted insurers to capture market share, and therefore loss experience data, allowing for more accurate pricing and eventually large and profitable lines of business. Once an understanding of cyber perils is obtained, underwriting criteria can be relaxed and these policies will be much more marketable.

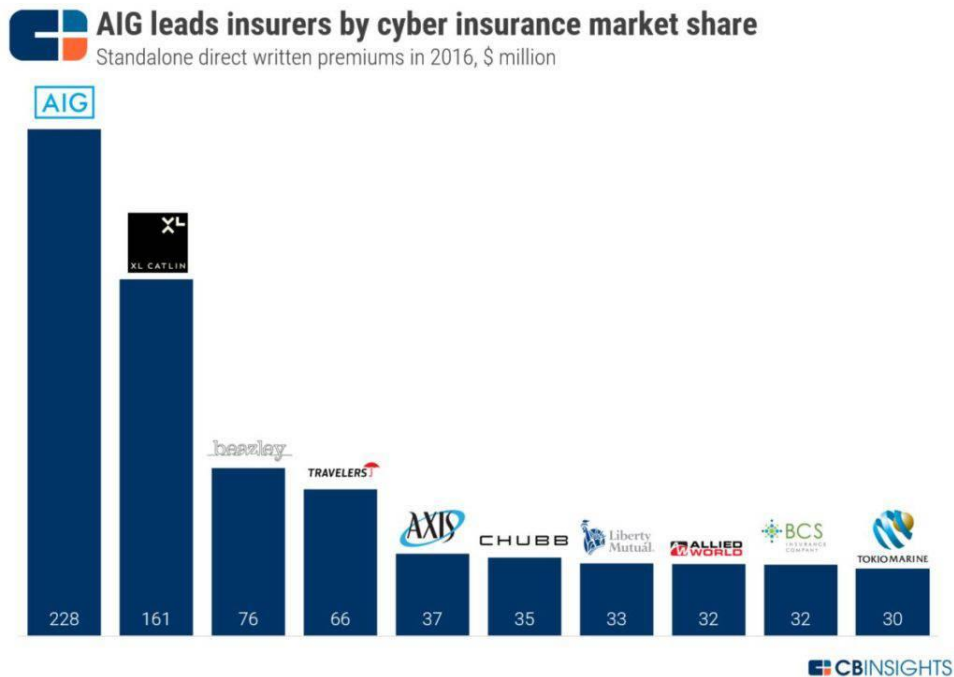


Figure 4. Image from CB Insights Research.

Interestingly, periodic large breaches can benefit the market as a whole. Growth in premium over the past few years can be partially attributed to the Yahoo, Equifax, and Target breaches and the media coverage surrounding them (Lenihan). Increasing public awareness to threats posed by breaches and other data protection failures will only help carriers increase their cyber business moving forward. Where there is risk, especially non-traditional risk, the non-admitted insurers will step in to provide coverage and offer stable market to their customers.

Conclusion

Cyber insurance is a line still in its infantile stage. Risk aversion from insurers is hindering the potential desirability of this insurance for businesses, as well as the availability of data to properly price and reserve. Limits are too low for many companies, and the exclusions and requirements mean that cyber insurance also requires continuous costly IT upgrades. A proactive approach would be to accept a variety of exposures to learn about different risks associated with individual industries.

Capturing market share early could potentially sacrifice short-term profits but the knowledge acquired would be invaluable. Non-admitted carriers have the resources to innovate and create customize contracts that give them an underwriting edge over admitted carriers.

Creativity and dexterity to adapt with emerging trends is an attribute of the non-admitted market that will be a vital asset in the growth of cyber insurance. Insurers can contribute to the advancement of cybersecurity by advocating for better data protection standards. By taking advantage of their role as risk managers, insurers can branch out to provide additional services to

aid in the cybersecurity of their insureds, which could distinguish them from the competition, and allow them to become leaders in the market.

Works Cited

@DMBisson, David Bisson Follow. "Average Organizational, Per Capita Data Breach Costs Reach New Highs." *The State of Security*, 20 June 2017, www.tripwire.com/state-of-security/security-data-protection/report-average-organizational-and-per-capita-costs-of-data-breach-reach-new-highs/.

AIG, Chubb, XL Group Lead in U.S. Cyber Coverage Market Share: Fitch Ratings." *Insurance Journal*, *Insurance Journal*, 1 Sept. 2016, www.insurancejournal.com/magazines/features/2016/09/06/424904.htm.

American International Group. "Cyber Insurance." *Cyber Insurance for Businesses*, AIG, www.aig.com/business/insurance/cyber-insurance.

"Analyzing the Evolution of AIG's Cyber Insurance Offering." *CB Insights Research*, 22 Feb. 2018, www.cbinsights.com/research/aig-cyber-insurance-expert-intelligence/

"Cyber Insurance Premium Volume Grew 35% to \$1.3 Billion in 2016." *Insurance Journal*, 22 June 2017, www.insurancejournal.com/news/national/2017/06/23/455508.htm

Greenwald, Judy. "Specialty market keeps grip on cyber risk." *Business Insurance*, 24 Oct. 2016, 12:00 AM, www.businessinsurance.com/article/00010101/NEWS06/912310137/Specialty-market-keeps-grip-on-cyber-risk.

Kesan, Jay P, and Ruperto P Majuca. "The Economic Case for Cyberinsurance." *The Berkeley Electronic Press*.

Lenihan, Rob. "High-Profile breaches to drive cyber insurance uptake: Fitch." *Business Insurance*, Business Insurance Holding , 27 Sept. 2017, www.businessinsurance.com/article/20170927/NEWS06/912316108/High-profile-breaches-to-drive-cyber-insurance-uptake-Fitch.

Martin, Taylor. "How to Fix the MacOS High Sierra Root Password Bug." *CNET*, CNET, 29 Nov. 2017, www.cnet.com/how-to/how-to-fix-the-macos-high-sierra-password-bug/.

NCSL. "Security Breach Notification Laws." *National Conference of State Legislatures*, National Conference of State Legislatures, 29 Sept. 2018, <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> NetDiligence. "2016 Cyber Claims Study ." *NetDiligence*, NetDiligence, 17 Oct. 2016, netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf.

O'Hearn, Stephen, et al. "Insurance 2020 & beyond: Reaping the Dividends of Cyber Resilience." www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

Ponemon Institute. *2017 Cost of Data Breach Study*. Ponemon Institute & IBM Security, June 2017, public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/SEL03130WWEN.PDF.

Schoenberg, Carter, and IDG Contributor Network. "Cyber Insurance in the 2018 Regulatory Landscape." *CSO Online*. CSO, 16 Jan. 2018. Web. 30 Oct. 2018.