Journal of Reinsurance 2019

IRUA

Volume 26
Number 1

In This Issue:

Insuring Against Unknown Cyber Attacks in the Age of IoT

2018 First Place IRUA Summer Intern Scholar Awardee

By Luke M. Schwenke, Data Science Intern, Markel Corporation

About the Author

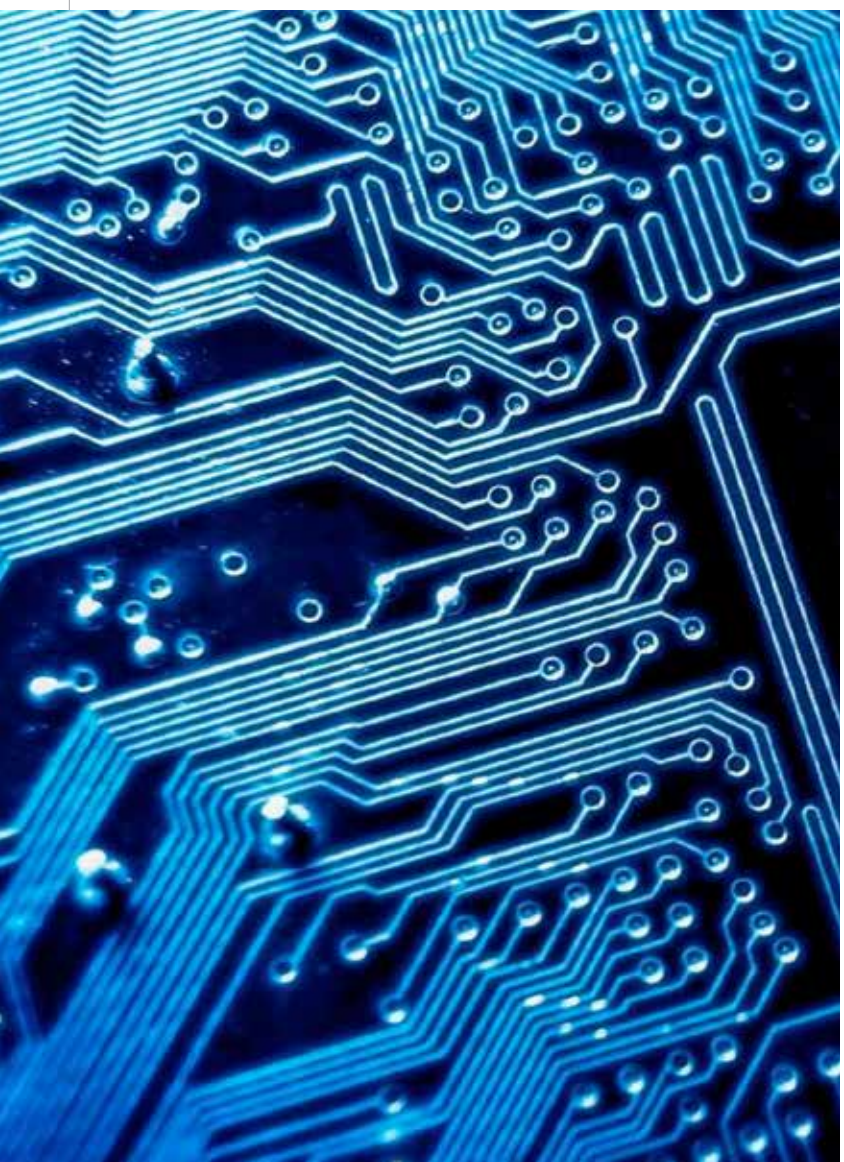
Luke M. Schwenke was the first place winner in IRUA's 2018 Scholars Essay contest. He interned during the summer of 2018 with Markel Corporation and will graduate in May 2019 from the College of William & Mary with a B.S. in Data Science and a minor in Arabic Language & Literature. He will begin working with Markel Corporation, once again, as an Associate Data Scientist.

Abstract

"To me, the elephant in the room today is what we call the 'cyber' issue. The growing interconnectivity of computers, their ability to learn from each other and the fact that the world's economy has become absolutely dependent on the internet raises huge new challenges for the insurance industry."

-Stephen Catlin, XL Group Ltd

The introduction of IoT technology is both exciting and significant for the (re)insurance industry. It is changing the way insurance companies write business and is challenging reinsurance companies to think about different approaches in covering new technology. Alongside IoT's power and ease of connectivity between devices, there are also endless vulnerabilities that leave people exposed to cyber attacks at any point in time. This paper will provide an in-depth look into the types of IoT that exist, its role with insurance and impact on (re)insurance, and its challenges/solutions for the industry as a whole. This paper gives a wide-breadth of first-hand insights from personal interviews as well as information from scholarly articles in order to accurately communicate the difficulties of insuring against unknown cyber attacks in the modern technological world. It will conclude by offering solutions to the difficulties companies and organizations are experiencing, and discuss the benefits IoT technology is having and will have on the industry.



RELEVANCE

The chance of an unknown cyber attack occurring happens at every moment in our technology driven world. Individuals, small businesses, corporations, and nations are attempting to adapt to this environment and are willing to spend billions of dollars to do so.

Gone are the days when serious damage was only done with things such as bombs and soldiers on the ground; the replacement is cyber warfare, where people can cause serious harm thousands of miles away, or right down the street, without anyone really noticing what has happened until after the damage is done.

With the introduction of IoT technology, the risk of a powerful cyber attack is exponentially greater because of its connective power between devices and the people's lives who own them. IoT and its cyber security implications are important to discuss because it is the future of nearly every industry.

Companies are going to have to adopt these technologies in order to stay competitive in the long run and the only way to be successful will be to prepare for the inevitable unknown cyber attacks and software glitches.

CHAPTER 1 DEFINING IoT

IoT stands for the Internet of Things, but is also commonly referred to as the Internet of Everything. IoT is a new technology paradigm that can be envisioned as a global network comprised of machines and devices. Devices in this network are capable of communicating with each other in a seemingly infinite number of ways to enhance day-to-day life. It is recognized as one of the most important areas of future

Continued from page 3

technology and has been gaining vast attention in many industries, one of which is insurance.

IoT has a lot of potential but there are also innumerable risks involved; that is where (re)insurance comes into play. Organizations will need to be able to mitigate as many risks as possible so they do not lose exorbitant amounts of money that could cause bankruptcy or ruin lives. Insurance will be able to provide the necessary peace of mind to organizations implementing IoT technology so they can continue to take on new and exciting risks that will further grow their prospective ventures and, develop their industry and economy as a whole.

CHAPTER 2 TYPES OF IoT

According to Gartner, a leading research and advisory company, IoT usage will increase 2,788% from 0.9 billion units in 2009 to 26 billion units by 2020. Additionally, companies are expected to invest over $6 trillion in IoT solutions in the next five years (Chordas 2018).

IoT has its hands in every industry from production line and warehousing to retail delivery and store shelving. Firms plan on investing in IoT to redesign factory workflows, improve tracking of materials, and optimize distribution costs. For example, John Deere and UPS are using IoT-enabled fleet tracking technology to cut costs and improve supply efficiency. Various service industries are also using IoT to increase revenue through enhanced services. Disney's MagicBand includes a chip that serves as a ticket and connects to Disney's data repository regarding park visitors. Kroger has a new system that combines video analytics, wireless Point of Sale (POS) devices, handheld sensors, IP cameras, and video management software that helps customers have a better shopping experience by assisting them in finding products and cutting checkout times. Overall, IoT is based on 5 overarching technology types that are listed below (Lee, Lee 2015)

Aside from commercial use, IoT technology is also being implemented in homes across the world. The term "smart home" is at the forefront of innovation regarding monitoring and control systems. These technologies primarily find value in family and property protection as well as energy savings. Tyler Joiner, Team Lead of Data Analytics at Markel Corporation, describes some of the risk associated with two popular smart home products. The first is a smart thermostat called Nest that has the capability of being controlled from your smartphone. Nest's company advertises the device can adjust temperatures when you're away, can pay for itself in two years or less, can be controlled from anywhere, and has remote temperature sensing to adjust certain rooms to specific temperatures (Nest.com 2018). Joiner explains that someone could hack into the app on her phone and easily be able to discern her family's day-to-day schedule based on the temperatures. For example, in the summer, the temperature of the house will increase during the day when nobody is home since there is no need to cool an empty house.

Essential IoT Technologies

- **Radio Frequency Identification (RFID)**
- **Wireless Sensor Networks (WSN)**
- **Middleware**
- **Cloud Computing**
- **IoT Application Software**

Another example Joiner provides is with smart refrigerators. These refrigerators are able to detect the type of items stored inside and keep track of important details such as expiration dates and usage through RFID technology that matches the bar code with manufacturer details directly from the internet. Joiner says, "A hacker could tell, based on items in the refrigerator, what type of person they are. A refrigerator with beer, milk, and eggs is most likely a college student whereas a refrigerator with higher-priced non-necessity items, such as kombucha, may reveal someone with more expendable income." The extra information these new devices provides increases the consumer's exposure to danger. (Joiner 2018)

Kyoochun Lee and In Lee's, "The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises", shows how IoT is penetrating retail, manufacturing, healthcare, home appliances, heavy equipment, airlines, and logistics. "The benefits of IoT technologies such as RFID-based merchandise tracking and home networking are concrete and immediately measurable". It appears that other technologies, such as automobiles and intelligent hospital robot systems, are more experimental in nature so their benefits may not be realized for a few more years. Despite IoT being relatively new, there are copious investment opportunities that companies are expected to take advantage of with new waves of IoT innovation.

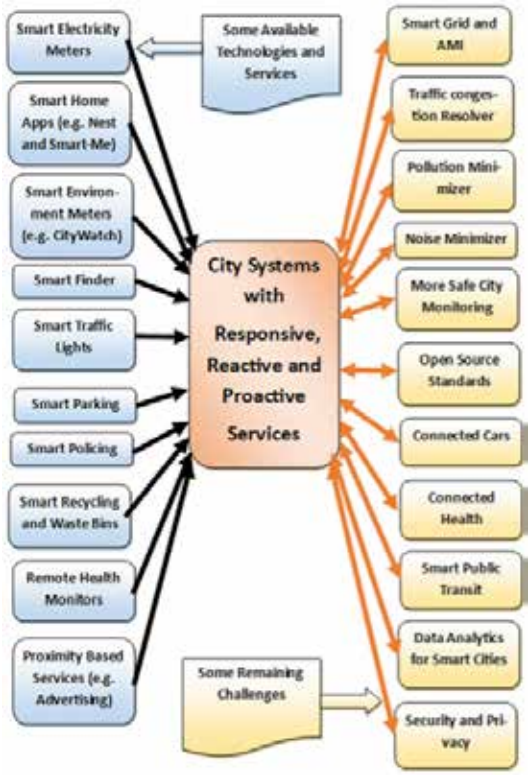
> **"Ignorance of future risks and procrastination over taking action are never solutions."**
>
> **-O'Brien**

CHAPTER 3 ROLE OF INSURANCE

There are endless scenarios where cyber insurance is needed to cushion against breaches in IoT technology. Michael O'Brien, a partner at the law firm Wilson Elser Moskowitz Edelman & Dicker, gives an example of a loss scenario: "Say a factory suffers an electrical fire from a malfunctioning piece of equipment. Now, assume the investigator of the fire's cause and origin and the supporting forensic engineers determine that the most probable cause is the IoT enablement of the equipment. In the post-fire forensic investigation, evidence emerges that someone had hacked into the sensors and operational controls in the equipment that measured heat, sending erroneous information via the internet, which resulted in overriding the critical safety controls of the machinery, causing the electrical fire." (Banham 2016)

This electrical fire example (See Fig. 1) illustrates just one scenario of an IoT cyber attack. What if this electrical fire was induced on a much larger scale or in a densely populated area? The diagram below shows how cities such as Padova, Italy and Tokyo, Japan are working on implementing these

Figure 1



technologies into every aspect of their domain (Lee, Lee 2015). The imagination is the only limitation as to the amount and type of security breaches that can occur in a scenario where a whole city is connected.

Some cyber coverage is available as an add-on to existing policy types (e.g. Commercial General Liability) and covers typical errors, data thefts, and extortion. Despite these add-ons, there are still coverage gaps for standalone cyber security insurance that reveal the opportunities to expand into this space and its necessity for companies and organizations. (Oxford Analytica)

Insurance companies and brokers are beginning to understand the dramatic changes to the risk landscape. People tend to think the main reason for cyber insurance is protecting data privacy, but there are other aspects that are equally, if not more, important to think about. Robert Parisi, Managing Director and Cyber Product Lead at Marsh Inc., believes, "the question of whether or not these insurance terms and conditions address IoT-related losses is one of the most interesting issues in the marketplace right now". There is a lot of debate as to what type of insurance policy will even cover these types of risk -- will it reside with a cyber, property, or some other policy?

Technology is a constantly evolving threat, and underwriters will have to enhance their understanding of IoT risks if they want to add them on their balance sheets.

Ethical hackers have been utilized to demonstrate vulnerabilities in certain products. Security researchers were able to hack into the dashboard computer of a Jeep Cherokee and take control of the vehicle. From this point, they could steer the car, as well as adjust the transmission and brakes to speed up or slow down the vehicle. Fiat Chrysler, the parent company of Jeep, ended up recalling 1.4 million vehicles because of this vulnerability. If the hackers' intent had been malicious, there may have been substantial loss of life, bodily injuries, and property damage. The affected drivers' automobile insurance would probably cover some of the financial loss, but that,

> "There's always the concern that technology can be misused and the knowledge that it will be misused."
>
> -Gorski

"would be the first domino in a long liability chain as the insurers might then sue other culpable parties to recoup their losses" (Banham 2016). These complex claims are challenging because it can be hard to pin down who is liable for what part of the process. It will be important for insurance companies to set concrete guidelines as to what this will look like.

A July 2014 study by Hewlett Packard reveals 7 in 10 IoT devices contain vulnerabilities. Moreover, "70% of the sensors did not encrypt internet or local network communications; half performed encrypted communications to the cloud, internet or local network; and 80% failed to require passwords of sufficient complexity and length" (Banham 2016). Al Gorski, Chief Risk Officer for the transportation authority in Orange, California, knows the potential for IoT systems to be hacked and create liability issues.

He says, "There's always the concern that technology can be misused and the knowledge that it will be misused". Since many industries are looking to take advantage of the benefits of this interwoven world, a single insurance solution will not be enough. It will be too hard to implement a one-size-fits-all policy. Some of the possible insurance policies needed to supplement cyber insurance include (1) technology errors and omissions insurance to cover 3rd party claims made by clients for inadequate work or negligent action in providing technology services/products, (2) product liability insurance to cover 3rd party claims due to damage to property containing a defective product, and (3) product recall insurance to cover 1st party claims due to recalls. (Angrishi 2017)

Innovative risk transfer solutions will be generated, particularly in relation to existing policies, as insurer awareness of the risks of IoT increases. Michael O'Brien elaborates on this topic and says, "as this awareness grows and insurers begin to address the potential for large- scale internet-based losses resulting in property damage or bodily injury or both, the industry will adjust by developing policy exclusions or endorsements, while grappling with trying to determine how much risk to take and what premium to charge for this risk". (Banham 2016) Note: This challenge, along with others in the (re)insurance industry, is discussed in Chapter 5.

Adwait Nadkarni, Assistant Professor of Computer Science and specialist in IoT research at the College of William & Mary, explained there are 3 key parts of technology that need to be kept in check for IoT to be implemented successfully.

- **Confidentiality:** devices should keep sensitive information private.
- **Integrity:** devices should provide consistent and accurate reports.
- **Availability:** devices should be up to date and free of software conflicts.

Professor Nadkarni claims it can be challenging to maintain all of the key parts but, "it will be critical for IoT to be secure because the stakes are much higher". He gave an example of these intense circumstances where the financial and human costs are very high in the medical field. IoT

Continued on page 6

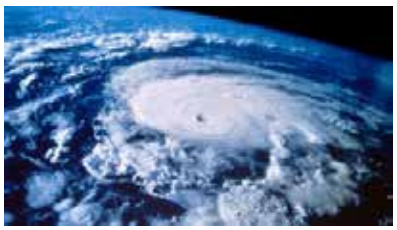
Continued from page 5

devices are being implanted in people to measure vital signs such as blood pressure or heart rate (see below). A deviation from the true results or a glitch in the software could cost the person his/her life. This leads to an even greater need for insurance. Additionally, Professor Nadkarni believes IoT technology insurance actually fits quite well into the current business model. He describes that such accidents as mentioned above may not happen frequently but their aftermath can be expensive. This is similar to how the airplane industry has developed.

Since 1950, the number of airline accidents has decreased from a 5-year average of around 80 to 22 or so by the year 2015. Despite this incredibly low number of accidents compared to the 15,631,000 flights handled by the Federal Aviation Administration in 2016 alone, airlines still pay a lot of money for insurance because the fallout can easily climb into the upper millions of dollars. (faa.gov 2017) In the coming decades, we may expect a similar trend with IoT where a lot of cyber attacks or bugs are occurring in the beginning but begin to decrease in the long run as improvements are made and security effectiveness has increased. This is not to say though that the need for insurance will diminish since the danger will still exist and is likely to be high in the coming decades.

CHAPTER 4

IMPACT ON REINSURANCE



Because of the development of IoT technology and the potential for cyber attacks, it can be expected that this type of insurance will increase dramatically. Interestingly, alongside an increase of cyber insurance, the overall world of risk in the insurance realm will transform. Steven M. McElhiney, CEO of Dallas-based EWI Re, explains that, "industrial explosions and marine accidents may soon become almost nonexistent because of sensors and proactive monitoring" (Chordas 2018).

From this quote, it appears there will be a shift in terms of the claims insurance companies will be paying out. While cyber insurance will be increasing and driving up costs, other areas such as industrial and marine will not have as many payouts. What is important though is whether or not there is a balance between these concepts. If cyber claims go up and marine claims go down, how much is the cyber actually going up? Based on the number of devices that will be connected, it would be easy to suspect cyber insurance will still have significantly larger premiums and claims.

If IoT technology creates the potential for large claims, reinsurance has a unique opportunity. Though not as predictable as natural disasters, like hurricanes that have cyclical seasons, cyber attacks could be equally, if not more, expensive and damaging than these events for a number or reasons, one of which being that they are not constrained geographically. It will be the job of the reinsurance industry to provide the coverage options that insurers need to effectively underwrite cyber risk exposures with the potential to have catastrophic claims.

> **"It will be critical for IoT to be secure because the stakes are much higher."**
>
> **-Nadkarni**

In September of 2017, Equifax had a cyber attack that exposed 160 million customers' Social Security numbers, home addresses, and drivers' license numbers. The attack cost Equifax $4 billion which could not be picked up by in full by their insurance companies. These insurance companies then had to turn towards their reinsurers. (GlobalReinsurance.com) Compared to events like Hurricane Harvey in 2017 that inflicted $125 billion in damages, this singular cyber attack seems minuscule, but in total, cyber related crimes are costing businesses $400 billion every year (Manral 2015). As more IoT devices connect to the network, the effects of devastating claims rise. Patti Titus, Chief Information Security Officer at Markel Corporation, explained in an interview the vertical impact IoT will have on the reinsurance industry. She specifically talked about the smart power grid of the United States and our country's move towards a more centralized infrastructure.

Titus says the interconnections between power grids will allow people to do serious damage that can rival that of hurricanes. Hackers would be able to "leap frog" from these power grids to devices inside companies or homes via their wireless network systems to listen in on conversations, plant malware, acquire sensitive information, or any number of nefarious intents.

Capsicum Re defines the term "non-affirmative cyber" to refer to instances where the cyber risk is not explicitly included nor explicitly excluded in the policy; similarly, "affirmative" means the risk is defined. In their 2017 article, "Addressing Non-Affirmative Cyber", Capsicum Re describes four current factors which are changing the dynamics of cyber insurance.

- **Increasing regulatory pressure.**
- **Increasing frequency of large cyber-attacks.**
- **Lack of uniformity of implementation of cyber exclusionary wording.**
- **Potential macro shift in the existing soft market dynamics.**

Regarding the first bullet, the expectations for companies are that they will need to adjust premiums to reflect additional risk and offer explicit coverage, introduce robust wording exclusions, and attach specific limits. As for the second bullet, Capsicum Re exemplifies the increase of larger cyber attacks through the 2017 WannaCry and NotPetya attacks that cost their prospective regions billions of dollars. In instances such as the Equifax breach, losses can cascade to other places such as Directors and Officers liability (D&O) even though affirmative cyber coverage is in place.

The third factor describes how lack of clarity can lead to ambiguity, unknown exposure for the insurer, and exponential aggregation for reinsurers. Clarity is paramount to the industry since insurance's core role is to ease

some of this risk and uncertainty away. Without the policy being clear and straightforward, it will be hard for policies to work correctly and cover unknown cyber attacks.

Finally, the fourth factor relates back to a point Patti Titus made. The only way to start a macro shift, where insurers begin calculating and accepting more risk exposures, is unfortunately with the occurrence of a large-scale attack or the potential for significant losses around the world. Additionally, reinsurers may also push back on including non-affirmative cyber policies in property or other classes of business.

Furthermore, Capsicum Re highlights the possible directions of the cyber (re)insurance market. These directions are:

- **Market remains unchanged.**
- **Underwriters gain the necessary knowledge for cyber.**
- **Affirmative cyber covers become consolidated with standalone policy offerings..**

If the cyber insurance market remains unchanged, the industry will continue to lack understanding of how to correctly price and assess non-affirmative cyber exposure. Additionally, there would be a potential increase in non-affirmative cyber exposures. This pathway will not be sustainable for the future and would leave many organizations vulnerable to large-scale cyber attacks and snowball into more problems.

Another direction is a shift towards affirmative cyber policies that cover non-affirmative exposures. This particular job would most likely fall to a cyber underwriter. This underwriter would be able to provide more accurate knowledge on how to best cover the policy. Additionally, combining affirmative cyber with their non-affirmative counterparts would clear up some discrepancy. Note: The second point regarding underwriter knowledge will be discussed in Chapter 5 as a principal challenge.

Kara Owens, Managing Director and Global Cyber Underwriting Executive at Markel Corporation, emphasized in an interview the effect aggregation will have on reinsurance. She explained how many of these IoT cyber attacks will hit multiple carriers across different product lines all at once. Combined with outdated contract exclusionary wordings, reinsurance companies will have a hard time figuring out the best options for policies to cover and how to approach them. In order to ameliorate some of these issues, reinsurers can work more closely with regulators and be proactive, rather than reactive, in their efforts to learn about IoT trends and patterns.

Owens also described how CAT modelers are beginning to look at IoT cyber attacks more closely by examining the effects disasters like a massive cloud outage would have. As IoT continues to develop, we can expect these disaster scenario models to increase in number to account for cyber attack possibilities.

Some affirmative cyber plans currently exist such as, Brit Cyber Attack Plus (BCAP) which has a capacity of $200-$350 million. This product was originally a Property Damage and Business Interruption cover but expanded to offer more covers such as cyber extortion, digital asset restoration, crisis management costs, system failure, and more. We can expect more products like BCAP to come to the market within the coming years as the necessity for higher capacities and wider coverage increases.

Overall, IoT's impact on reinsurance will be momentous while hopefully providing positive opportunity for change, growth, and learning. Reinsurers will need to be ready to cover insurance companies when large cyber attack claims start coming in. It will be important for companies to begin learning about the technology soon so they can both reap its benefits early in the game and prevent themselves from getting burned later on. Taking the step to add cyber attacks to CAT models is significant because it shows the industry is already taking the vulnerabilities seriously and is preparing for the future.

CHAPTER 5 CHALLENGES & SOLUTIONS

There are a lot of possible challenges that the insurance and reinsurance industries are likely to face in the age of IoT. Jessica Chang, Team Lead of Global Security Services at Markel Corporation, provided insight into some of these difficulties by speaking to her own experiences at Markel.

One of the main points she discussed was the need to hire expert consultants who are able to come into an insurance or reinsurance company to accurately measure risks and key factors. These experts will be vital in determining premium amounts and exposure for IoT technology. Current underwriters without knowledge of IoT will struggle to find ways to bring value to the company because of this lack of knowledge. There are a few solutions to this challenge. The first could be what Markel does frequently, hiring temporary experts who are able to provide answers to questions and fix problems that normal full-time employees are not able to. Though this is a fair solution, it may not be able to keep up with the rapid growth of IoT. A more effective solution for the long term could be to offer extensive training courses for current underwriters and employees so they can increase their own understanding of the subject. Even attending IoT conferences rather than hiring instructors could be a cheaper but still effective option for underwriters to learn about the technology.

These educational opportunities would supply underwriters with the robust tools they need to properly price premiums, and would, in turn, generate value for their prospective company in a more dynamic and versatile manner. For example, if they learn about an IoT product that uses radio frequency interaction (RFID), they could extrapolate their newly acquired knowledge and apply it to products they come across in the future that use similar technology.

Another challenge, which is understood by everyone in (re)insurance, is that these processes are slow-moving. The danger of unknown cyber attacks will continue to pose a serious threat, but until something calamitous occurs, the process of safeguarding against dangers will only inch along. Patti Titus said that based on her experiences, "It won't be a problem until it's already a problem" (Titus 2018). The solution to this, and to keep the industry thriving, has been a challenge in and of itself since the genesis of insurance. People will need to be educated more on why they need cyber insurance for their IoT devices. It is difficult to conceptualize the exact policy needed to protect against the myriad of devices, but it will be important for people to know that they need insurance for IoT. Advertisements or warning labels are two ways this may be accomplished.

Continued on page 8

Continued from page 7

"It won't be a problem, until it's already a problem" -Titus

Direct communication between technology manufacturers and insurers will also be vital so carriers have a better direction in developing products. If developers can properly communicate how secure their IoT devices are, insurance companies will have a better chance of accurately pricing the risk. Companies like Apple have greatly increased the effectiveness of their encryption services, specifically with how people unlock their Apple devices. They are so good that in 2016 the United States Federal Bureau of Investigation requested Apple to write new software that would allow them to unlock a terrorist's IPhone 5C. (Wikipedia 2018)

Mike Scyphers, Chief Information Officer at Markel Corporation, described how he has, "170 devices on WiFi at home and none of them are secure. We are certainly going to see interesting things happen in this space as people become aware of how insecure their devices are" (Scyphers 2018). For now, people are somewhat content with companies creating devices that do not have formidable security systems. This is beginning to change as people realize the risk and danger. A few months ago, an Amazon Alexa listened to and recorded a private conversation between a couple and accidentally sent it to one of their coworkers. It was not a malicious attack but it is easy to see the implications this could have if someone were to hack into an Alexa or a similar device that has audio or visual recording capabilities.

Professor Nadkarni described two of the challenges he anticipates for insurance companies. The first will be in defining who is liable when a claim arises. For example, if an autonomous car is hacked, does the blame fall to the car manufacturer or the company that created the software of the device inside? Professor Nadkarni says extensive research and expert knowledge will be necessary to solve this challenge. The second difficulty is deciding what to cover and what not to cover. Many current cyber policies exclude a lot of cases but the introduction of IoT technology will require companies to become creative yet reasonable in determining what should be covered. (Nadkarni 2018)

CHAPTER 6 BENEFITS

Despite these challenges, a lot of benefits will affect insurance and reinsurance with investments in IoT. Embedded sensors and other technologies will help companies gather data 24/7 about potential failures and accidents. This will allow them to anticipate a claim or failure before they even occur. Moreover, these updates can reduce physical investigations, and reduce loss adjustment expenses, as well as, speed up the claim settlement process. (Manral 2015) From these examples, periodic inspections will transform into "real-time" data gathering that will allow the industry to make significantly more accurate predictions. IoT technology could help larger, traditional insurance become more customer-centric with specialty products and services that appeal to younger generations in many ways.

Examples of this can already be seen on a smaller scale with insurtechs (companies that combine technology with insurance) such as Lemonade, a mobile-based renters and homeowners insurance company that uses premiums pooled from peer groups to pay for claims and gives leftover money to customers. The company is utilizing automation, behavioral economics, and machine learning to speed up their processes. This innovation is highly attractive to millennials because it shortens the time it takes to purchase affordable insurance and it saves them money, further strengthening the customer to company relationship. IoT technology will allow traditional insurance companies to stay competitive with these smaller

Lemonade

insurtechs and to distinguish themselves as just as relevant, innovative, and convenient. Mike Scyphers described how it will be useful for companies like Markel to allow smaller insuretechs to move into the IoT space first and then leverage their technologies and progress.

Allowing others to go first gives room to prepare and learn from others' mistakes and successes.

Perhaps most obviously, insurance for IoT technology glitches or cyber attacks will also provide another stream of premium income for companies. As mentioned, some of the types of policies and insurance needed may not have been created yet, but there will definitely be a space that needs to be filled. This space can be used as an opportunity for insurance companies looking to expand into a more dynamic and technologically modern sector of the economy.

CONCLUSION

The development of IoT technology is already causing major ripples across the global economy. As the number of devices continues to grow, we can expect the vulnerabilities of this intertwined network to increase significantly as people with malicious intent will be able to bounce from one IoT device to the next via wireless connections. Not only will it be necessary for developers to increase their devices' encryption capabilities, but insurance and reinsurance companies will have to create more policies and invent coverage variations that do not yet exist to cover a wider range of risks since a one-size-fits-all policy will not work. Insurance companies will have to educate their underwriters through conferences/training sessions or bring in IoT experts to help them accurately price the risk of these new products. The reinsurance industry will have to scale to a point that can accommodate devastating cyber attacks such as power-grid shutdowns or massive interruptions so it can support insurance companies affected by many claims at one time. Insurance underwriting will become more tailored to clients based on real-time information that is transmitted from IoT technology, and traditional systems will shift from a statistically- based rating process to one based on true exposures that vary over time. It is a very exciting time for the (re)insurance industry because processes will have the most up-to-date information possible which will allow analytics teams to provide accurate business insights that were not able to be discovered before. Awareness of the challenges of IoT, coupled with the optimism of its power and benefits, will bring a wealth of success to the (re)insurance industry as it enters the new mainstream of contemporary business. ◀

TEXT REFERENCES

"Air Traffic By The Numbers." FAA Seal, 14 Nov. 2017, www.faa.gov/air_traffic/by_the_numbers/.

Angrishi, Kishore. Cornell University: "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets." 2017. Banham, Russ. "IOT COMPLEXITY." Risk Management, vol. 63, no. 6, 2016, pp. 38-42. ProQuest, https://proxy.wm.edu/login?.

url=https://search.proquest.com/docview/1813906667?accountid=15053..

Bousfield, Patrick. Addressing Non-Affirmative Cyber. Capsicum Re, 2017, Addressing Non-Affirmative Cyber. "Case Study: What Can Reinsurers Learn from the Equifax Breach?" Global Reinsurance, 14 Dec. 2017,

www.globalreinsurance.com/analysis/case-study-what-can-reinsurers-learn-from-the-equifax-breach/1425838.article.

Chang, Jessica. "Personal Interview - Markel Global Security Services." 6 July 2018.

"College of William & Mary Databases." William & Mary Libraries, libraries.wm.edu/databases.

Chordas, L. (2018). Sky's the limit. Best's Review, (3), 50-53. Retrieved from https://proxy.wm.edu/login? url=https://search.proquest.com/docview/2008824651?accountid=15053.

Gartner, 2014 Gartner. (2014, March 19). Gartner says the Internet of Things will transform the data center. Retrieved from http://www.gartner.com/newsroom/id/2684616.

"INTERNATIONAL: Demand Will Outpace Cyber Insurance." Oxford Analytica Daily Brief Service, Aug 12, 2016, pp. 1. ProQuest, https://proxy.wm.edu/login?url=https://search.proquest.com/docview/1810887387?accountid=15053.

Joiner, Tyler. "Personal Interview - Markel Data Analytics." 6 July 2018.

Kim, et al. "Smart City and IoT." Future Generation Computer Systems, vol. 76, 2017, pp. 159–162.

Lee, I., & Lee, K. (August 2015). Business horizons (4th ed., Vol. 58, Pg. 431-440). New York, NY: Elsevier Science. Retrieved from https://www-sciencedirect com.proxy.wm.edu/science/article/pii/S0007681315000373#bib0025 .

Manral, Jai. Cornell University: "IoT Enabled Insurance Ecosystem - Possibilities Challenges and Risks." 2015. Nadkarni, Adwait. College of William & Mary: "Personal Interview - Professor of Computer Science." 11 July 2018. "Nest Thermostats | Keep You Comfortable and Help Save Energy." Nest, Nest Labs, Inc., nest.com/thermostats/?

gclid=EAIaIQobChMI39vxnvmC3AIVU1uGCh3wkQo5EAAYASAAEgIEXvD_BwE&gclsrc=aw.ds& .

dclid=CLr846L5gtwCFam_swodRPcP0Q. .

Owens, Kara. "Personal Interview - Managing Director and Global Cyber Underwriting Executive." 26 July 2018. Scyphers, Mike. "Presentation - Markel Chief Information Officer." 12 July 2018.

Titus, Patti. "Personal Interview - Markel Chief Information Security Officer." 6 July 2018.

"What Is a Smart Refrigerator? - Definition from Techopedia." Techopedia.com, www.techopedia.com/definition/15684/smart- refrigerator.