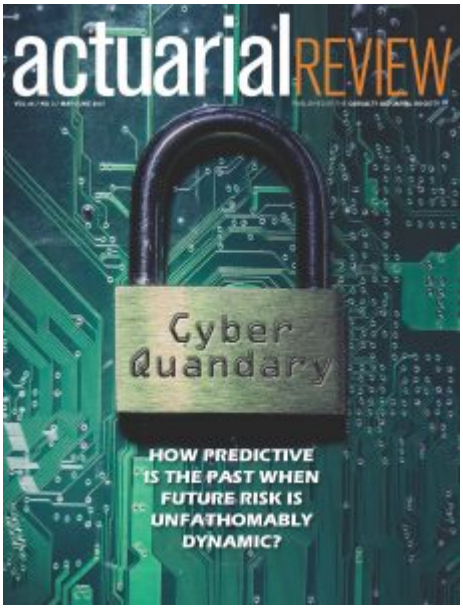
New Developments in Cyber Insurance Address Growing Needs



There are many new developments in cyber insurance.

Before the WannaCry worm began disrupting institutions all over the world last week, cyber insurers have been preparing for the rise in ransomware. This is among new developments in cyber insurance.

Insurers are also focusing on other cyber challenges, such as increasing risk from the connectivity of the Internet of things. As I point out in my recently published *Actuarial Review* article, Cyber Quandary, actuaries developing solutions to support the growing appetite for cyber insurance.

The article focuses on the latest developments in cyber threats and insurance, including emerging risks, market changes and innovative actuarial solutions. While emerging actuarial developments continue to progress, however, underwriting judgment still rules the day.

This is not surprising. Cyber insurance modeling is still very much in its infancy. It took more than a decade for personal auto underwriters, who tend to rely on experience and judgment, to adopt results from modern analytics.

After covering new developments in cyber insurance for the past three years, I marveled at how much cyber risk and insurance have changed. Consider the following:

- Americans, **once alarmed by headline-making data breaches** from department store credit cards, have accepted the likelihood of being breached thanks to hacks to health care insurers, internet sites and the federal government. Perhaps we feel helpless that we can't do much about it.
- **Ransomware** is **growing more popular.** As we are seeing with the WannaCry worm, bad actors find it profitable to hold information hostage – and they prefer payment a la Bitcoin.

- The **Internet of Things**, which increases cyber vulnerability, **was not yet part of the household lexicon** three years ago. While offering convenience, every connectivity point can be a weak link hackers can exploit. Consumers and businesses must take potential vulnerabilities from the Internet of Things more seriously.
- **Cyber insurance**, which centers on addressing costs from data breaches, **includes new coverages**, including manufacturing disruption due to greater connectivity.

- Two-and-a-half years ago, cyber insurance began growing in popularity. However, predicting losses was difficult due to the lack of historical data. Even as historical data becomes available, it has limited application due to the changing nature of risks. **Actuaries are finding new methods** and using non-traditional data **to enhance predictability**.

Meanwhile, there are other areas that deserve attention. These include:

- **Lack of policy standardization**. This makes it difficult for businesses to know exactly what coverage they need and what they are getting for their premium dollar.
- **Cyber hygiene and risk management neglect.** There are still too many companies — and people — who underestimate how basic security measures, such as updating software, can make a difference.

- **Personal lines insurers** are **slow to offer consumer cyber coverage**. I've been clamoring for this since my first cyber insurance article. Carriers can enhance their value propositions by offering consumers this vital coverage. There's always subrogation!

- **Preventing a cyber 9-11** and dealing with it if it comes, remains a great concern. Whether cyber terrorists compromise the Internet or utilities or God knows what else, all of us should prepare.

While there are many new developments in cyber insurance, I expect more to come. In the future, there will be more cyber insurance products that address specific industry concerns, additional options for small businesses and greater dependence on analytics for pricing and market segmentation.

To read my other cyber insurance articles, please click here.

Baribeau Offers Cyber Insurance Presentation

Last Tuesday, the Kansas City Actuaries Club honored me with an opportunity to discuss cyber insurance from a journalistic perspective.

The presentation included a market update, data breach statistics, underwriting practices, actuarial challenges and emerging cyber risks.

I greatly appreciate the Kansas City Actuaries Club for the chance to talk about this important emerging insurance line. Even better, all of them were great fun!

If you want to learn more about cyber insurance, check out my *Contingencies* article on the topic and look for my next article in *Leader's Edge* in May. I am also working on another cyber insurance article from the actuarial perspective for *Actuarial Review* for publication later this summer.

Also, remember to follow my blog so you won't miss any of my future articles. Just click on the "follow" button on the bottom right hand corner of this page.

Cyber Risk and Insurance Continue to Grow

Cyber risk and insurance continue to gain momentum. More companies realize they need it. And insurers are expanding coverage – and enjoying profitability. That said, cyber insurance continues to be an especially risky insurance line.

This is part of what I discuss in my recently published article, "Expansive Variance." Published in *Actuarial Review*, I titled the article very deliberately. The variance of risk expands in new ways every time I investigate cyber risk and insurance.

And frankly, the more I learn about cyber risk, the more concerned I become.

Cyber risk and insurance are expanding.

My article digs into the reasons behind the growing risk and new tools for actuaries and underwriters. Two particular trends stick out. First, Internet of Things technologies continue to introduce vulnerability to cyber attacks and personal privacy. Perhaps the best example of hacking through via app is last year's Facebook data breach.

Meanwhile, the bad guys, who have the creativity to walk the gauntlet of cyber protections, are quite innovative. Last year's Equifax breach, the largest in United States history, is a case in point. Despite tight cybersecurity, the breach pulled the personal data of more than 145 million Americans in a seven-week period. Another attack, less widely known to consumers, turned off factories and interfered with commerce all over the world.

The bad actors are also discovering ways to deploy artificial intelligence to mask coding to reach directly into personal computers. And for the less innovative, the old-fashioned and tried-and-true attack methods, such as email phishing, remain effective. Many companies still need to get religion on cybersecurity. Hackers are sometimes getting away with their dirty deeds because companies do not keep up with security patches.

These breaches serve as warnings of what could come. Everyone who knows about cyber risk and insurance fear "big one" — that cataclysmic breach that could put the world on its knees. Insurers are also very concerned about it, spreading risk across individual industries to reduce exposure.

Cyber Risk and Insurance

The article also describes the unique challenges insurers are facing beyond cyber risk itself. Currently, cyber insurance is generally profitable. The market is so competitive that it is sometimes underpriced. Executives of non-cyber insurance lines are also concerned that their coverages are picking up cyber loss.

Insurers have very different philosophies on covering cyber risk. For Warren Buffett, chairman of

Berkshire Hathaway, Inc., cyber risk and insurance just too risky. He believes that each year carries a 2% chance of a super catastrophe costing $400 billion or more in insured losses. Not surprisingly, his insurance group is mostly staying away from covering cyber risk.

But there's plenty of insurers – about 170 depending on classification – which are happy to offer cyber insurance. AIG and Chubb are two examples. Insurers also have more insurance scores for cyber risk than ever before. Depending on the product, such cyber scores can evaluate risk potential by company and can watch how the risk changes.

Privacy Regulations and Laws

Consumers have little remedy when personal data breaches occur. Cyber insurance covers cybersecurity protections for a limited amount of time, say two years or so. However, there is nothing that can be done to get the information back. The bad guys have it forever. Thankfully, cyber insurance for individuals is just starting to become available.

Last week I attended a seminar on protecting personal privacy sponsored by the Atlantic magazine and Salesforce.

Speakers discussed a social contract, which presumes entities collecting our data will protect it. However, this social contract has little law to support it. One privacy attorney says that the Facebook breach, while unethical, is not illegal.

The bad guys,
who have the creativity to walk
the gauntlet of cyber protections,
are quite innovative.

Americans assume the government is making sure our data is respected and kept private. But in truth, our public policymakers are behind the curve. As someone at the seminar joked, "Europeans regulate what Americans innovate." Legislative remedies are being considered by Congress. During the seminar, Senator Mark Warner (D-VA) mentioned a recent hearing where the nation's largest search engine's representatives were notably absent. The company, however, *is* showing up to help China with their internet although its employees are protesting and some have quit. This is the country that is following every move of their citizens to determine their "trustfulness" and is also blamed for particular cyber breaches.

My article describes new regulations from the European Union that affect American companies. California also passed an aggressive law to protect consumers. It goes into effect January 1, 2020. Not surprisingly, technology companies are fighting the restrictions the new law will impose. After all, they need personal data to sell ads. The European and California laws have potential ramifications for cyber insurers, but those details are yet to come.

Note: My last article about cyber insurance discusses particular challenges for actuaries. To see more of my cyber articles, just enter "cyber" in the search bar below.

Insurance Brokers Find Cyber Coverage Complex

While the cyber insurance market is booming, insurance brokers find cyber coverage complex.

Customers want to either get a cyber policy for the first time or boost their coverage through higher limits and more endorsements.

Insurance companies are very eager to sell various forms of it.

But that does not mean buying and selling cyber coverage is easy. As I explain in my recent *Leader's Edge* article, "**Confusion Reigns**," cyber insurance is going through the growing pains of a burgeoning insurance line.

Since the policies offered by 45-plus insurers are not standardized, the market offers a myriad of potential endorsements that range from data breach coverage to reputation damage to cyber extortion. This makes cyber coverage complex.

———————

…agents and brokers have to carefully comb through each policy to ensure the coverage matches the customer.

———————

And while there is growing demand for higher limits of insurance protection, agents and brokers sometimes have to layer coverage for their customers while keeping a close eye on various exclusions.

Because brokers and agents find cyber coverage to be complex, it also means they have to carefully comb through each policy to ensure the coverage matches the customer. And while insurance buyers should always be well informed about the coverage they are buying, this is especially true for cyber coverage.

I hope you enjoy it! Also, if you want to read more, check out my *Contingencies* article, "**Plugging the Data Breaches**."

Note: In July, I will be publishing a new article that looks closely at the actuarial challenges of cyber insurance. I'll let you know when my article is published, as I always do.

Be the first to know!
Just click the "follow" button
on the bottom right hand side of this blog.

Cyber Coverage Is Unprofitable, Now What?

Cyber coverage was once very profitable.

But that is no longer.

As I report in my recent article, Cyber Challenges, the growth of ransomware attacks and undisciplined underwriting practices are pressuring a line already considered too risky for most insurers.

The line's overall unprofitability was bound to happen. Sooner or later, profitability challenges hit every insurance line. That can be positive in the long term. Low returns on investment can motivate necessary soul searching that leads to growth and development.

To be clear, a line's overall profitability is not indicative of an individual insurer's experience. Some insurers are still making a decent buck selling cyber insurance. To stay in the cyber game, however, less profitable competitors are likely looking to reduce what they cover or quit offering coverage altogether.

Cyber insurance has always been risky business. Pricing coverage is challenging amid ever-changing risks. Since I began covering cyber insurance in 2014, data breaches were insurers' main concern.

But that changed.

Changing Risk

In 2018, data breaches continued to be the top concern. Ransomware was beginning to raise its ugly head. Back then, cyber coverage was also quite profitable. With losses at only 40% of expenses, there was plenty of room for double-digit profitability.

Now, cyber actuaries, charged with developing rates with little past or present data, are finally getting enough information to anticipate losses associated with data breaches. Actuaries have also become more sophisticated with scenario planning.

Despite these improvements, pricing cyber remains a delicate matter. Since cyber insurance was profitable, underwriters had some wiggle room for pricing coverage. But not anymore. Tighter underwriting, it is hoped, will result in organizations "getting religion" on risk mitigation. Recent

harrowing ransomware attacks, such as the Colonial Pipeline's, should serve as a wake-up call as well.

Battling cyberbullies is part of the price we pay for digital dependence.

Monitoring cyber insurance continues to be a challenge. Yes, there is plenty of data about cyber security. That, however, is only the risk side of the insurance equation.

While writing this article, I was surprised that after a three-year hiatus from covering cyber insurance, only one organization provided an estimate for the combined ratio — the insurance industry's go-to profitability barometer. The little publicly data available was laden in grains of salt or caveats as with sources warned the information does not paint a full picture.

Cyber insurance is important for protecting organizations when if a cyber attack occurs. Improving cyber security is vital, but so is building stronger partnerships between insurers and their customers. That critical piece could turn out to be the most important.

For Insurance, Predictive Modeling Will Surpass Human Judgment

Predictive modeling will surpass human judgment.

Predictive modeling will surpass human judgment and lead insurers to adapt a data and analytics insurance business model. This is according to sources in my recently published covering the latest in predictive modeling.

Published in the March/April issue of *Actuarial Review*, Predictive Prudence, also covers how the

new business model works, impediments limiting predictive modeling to reach full potential and data ethics.

Despite continual issues with data quality, information accessibility and regulatory considerations, predictive modeling is already demonstrating its power for guiding executive decision making, sources explain. As property-casualty insurance companies grow smarter in addressing predictive modeling barriers, some forward-moving carriers are already finding that predictive modeling can provide probability insight for decision-making and encourage measurable accountability.

Transitioning from a human judgment-based decision making to one based on models is not easy. The idea that predictive modeling will surpass human judgment is a threat to employees comfortable with traditional approaches. It is not surprising that internal pushback is a major reason why many insurance companies struggle to adapt to the new business model to remain competitive.

The idea that predictive modeling will surpass human judgment is a threat…

This article is part III in my series on the latest in predictive modeling. I am thrilled to see it spur discussion on Actuarial Outpost. The intent of three part series was to update actuaries on predictive modeling applications for varying lines and purposes. The first article covers growing data availability. The second one discusses the great modeling experimentation taking place for applications.

Here's the summary of the three articles:

1. **More data is available.** Ensuring data quality and obtaining enough of the right data to answer a question continues to be a growth area, especially for some commercial lines. Additional data is still needed.
2. **There are hundreds of potential models.** Actuaries and other quantitative professionals are experimenting with different ones to determine which will provide the most insight.
3. **Classic predictive modeling** through generalized linear modeling and decision trees are finding new applications. Concurrently, models beyond those, such as neural networks and gradient boosting, remain in the experimentation phase. There are traces of evidence that such models are being used in the real world.
4. **Predictive modeling will surpass human judgement** as it moves from specific, functional applications. Four years ago, I saw this potential and called it "integrated predictive modeling" in an article I wrote for the American Academy of Actuaries' *Contingencies* magazine.

Modeling Nomenclature

As a professional communicator who writes about actuarial topics and has worked with actuaries for 25 years, I urge the actuarial community to develop and adopt consistent nomenclature. Common nomenclature is unifying and quite practical. It is cumbersome to define terms just to have a conversation.

For example, I reluctantly choose to use the term "advanced modeling" to describe models beyond GLMs and decision trees because other terms are clunky. It's not a perfect term, I know.

Agreeing upon nomenclature will not only improve communication among actuaries, but the lay professionals that hire and depend on actuaries. Further, classifying models by type or family would

also aid discussion.

Another Article Coming!

In the coming months, I will also be publishing a piece in *Actuarial Review* describing how actuaries are addressing cyber insurance.

Question: Do you think predictive modeling will surpass human judgment for insurance decision-making? Please let me know by commenting below.

Q & A: Insurance Information Institute's Robert P. Hartwig

Robert Hartwig

Robert P. Hartwig, president and CEO of the Insurance Information Institute (III), has been one of my most valued sources for facts and opinions about this often misunderstood industry.

Hartwig is leaving in August to become a faculty member and co-director of the University of South Carolina's Moore School of Risk and Uncertainty Management Center. Hartwig, who has a Ph.D. in economics, also has a Chartered Property Casualty Underwriter designation.

Hailing from Oxford, Mass., which he describes as a one-traffic-light town during his youth, Hartwig has an impressive resume that includes key positions at Swiss Re, the National Council on Compensation Insurance (NCCI) and the U.S. Consumer Product Safety Commission. Hartwig joined III as its chief economist in 1998 and became president in 2007.

As a reporter, I first interviewed Bob while he was working at the NCCI 20 years ago. My first truly

Hartwig experience, however, took place when he sent me a 75-page "Drink From My Firehose" presentation as a basis for interview questions. As I was drowning from the waterfall of information, Bob helped me work through the pertinent material for an article.

True to his ever-helpful and insightful nature, Bob shared a few moments to talk about his views on the insurance industry, why he is joining the ranks of academia and more . . . .

Question: In the midst of traveling 150,000 miles annually, offering presentations and answering media calls, what do you do in your personal life?

Answer: I am an avid traveler and love seeing new places and experiencing different cultures. My job at the III has allowed me to travel all around the world, but I usually don't have a chance to soak up any of the local experience. On a recent business trip to Germany, for example, I was on the ground for a total of seven hours. On a trip to Beijing, I was there for a total of 14 hours. In my next career I hope to be able stay awhile!

After I arrive in South Carolina, I intend to get back into piloting airplanes. Ironically, because I was traveling so much for the III, there was no longer any time to fly on my own.

Question: What do you miss the most about flying airplanes?

Answer: Flying airplanes is not only exhilarating but it commands 100 percent of your attention. You think about nothing else other than flying the aircraft. It gives me an adrenaline rush and at the same time allows me to forget about everything else!

Question: Why did you go into insurance?

Answer: I've always been a numbers person and have had a lifelong fascination with statistics. I had a great opportunity back in 1993 after finishing my Ph.D. to work in the actuarial group at NCCI. It was the total immersion method of learning insurance but I wound up loving it.

Question: What has been your most fulfilling role so far in your career?

Answer: I love defending the industry against its critics — be it the media or on Capitol Hill. I enjoy the challenge. The insurance industry has a noble and necessary mission, but one that too often misunderstood or deliberately mischaracterized.

I've also love being a part of the industry in the aftermath of major disasters. With my office being in lower Manhattan, I had a real-time front row seat to the devastation and horror of the 9/11 attacks and was very proud of how this industry helped New York City and the country overall recover from those attacks. The industry truly fulfills its role as the nation's "economic first responder." The same is true after numerous other devastating events, including Hurricane Katrina and Superstorm Sandy.

The insurance industry has a noble and necessary mission,
but one that too often misunderstood or deliberately mischaracterized.

Question: As you think about the insurance industry during your career, what is going well?

Answer: Despite opinions to the contrary, I think the industry has adjusted fairly well to rapidly

changing nature of risks in the global economy.

My nearly 25 years in the industry began shortly after Hurricane Andrew in 1992, which became the most costly natural global at that time. The industry has adapted well to not only more frequently and costly natural catastrophes, but also the new risks of the 21st century.

Insurers are also rapidly ascending very steep learning curves for new risks such as cyber, supply chain, intellectual property, the "sharing economy" and the "internet of things." It's a brave new world, but all signs point to industry seizing opportunities and providing the risk management solutions that businesses and people need for the decades ahead.

Question: Where does the industry still need improvement and where do you have concerns?

Answer: While the industry is moving in the right direction in terms of offering underwriting and risk management solutions for the 21st century, advances in technology and data analytics potentially threaten to disintermediate the industry from its life's blood—the flow of information from customers and producers to the insurer.

Any interruption of this flow would also threaten insurers' role as the analytics engine that supports the pricing and underwriting of risk. Insurers have the edge, but need to beware of potential usurpers seeking to upend the insurance industry's value chain.

Question: Thanks for being such a reliable source for insurance information. I hope you will still accept media calls.

Answer: I'm looking forward to working with media in my new role in addition to continued interaction with the many stakeholders of this vital industry.

(Note: Starting Aug. 8, III's new top leader will be Sean Kevelighan. To learn more, click here.)

Facing the Insurance Quality Content Dilemma (Part 1)

To offer expert insurance content, insurance marketing and communications executives find their options are

CC0 Public Domain

hiring agency counterparts who do not deeply understand the intricacies of insurance or internal subject matter experts who do not want to become writers.

The dilemma is the direct result of two primary factors. First, there are few professionals who offer insurance expertise and possess audience-focused communications training and experience.

Second, effective marketing heavily relies on producing magnetic and substantive content. Amidst intensifying online competition, the C-Suite asks their internal marketing and communications departments to become publishers of brand journalism without the additional resources to support the effort.

Often, the C-Suite commonly does not want to accept that publishing is expensive. But it is. This is why so many newspapers and magazines, even those offered online, no longer exist. In a world of free content as a marketing approach, there is no option to sell advertising to underwrite the expense of professional communicators.

Without understanding the audience,
inbound marketing will fail.

Those who appreciate and understand insurance tend to be professionals whose aspirations didn't include becoming writers. Experts in claims management, underwriting, risk management, actuarial, statistics and other disciplines often despise writing. They began their careers not knowing that branding and digital marketing would introduce the publish-or-perish mentality that academics have struggled with for decades.

Such professionals are being asked to work beyond their skill sets while trying to maintain their core competencies through endless hours of continuing education. So it is not surprising that producing content by writing white papers or blogs becomes a hassle amidst their already busy days.

These experts find the writing process to be quite frustrating. After staring at a blank screen for seemingly hours, their material is often unorganized or too complicated, making it difficult to read and understand. As a result, the marketing and communications department must invest in heavy editing and re-writing. It's a time consuming and difficult process that can breed resentment on both sides.

Further, this approach is likely more expensive. Asking highly-paid professionals to write diverts their time and focus away from meeting client needs or rainmaking. Unfortunately, the C-Suite often does not take all these factors into consideration.

Lacking Insurance Expertise

The other option is to hire public relations, marketing and other communications firms. Usually, these well-intentioned companies lack deep and thorough insurance expertise.

The reality is that it takes years to understand the nuances of insurance. The industry not only has several disciplines, but several functions and a multitude of insurance lines. This makes finding expert insurance content writers even more difficult.

Workers' compensation, for example, involves understanding different subjects including health care, the claims process, return-to-work and disability coverage. Additionally, each state has its own regulations and expectations. Personal auto, the largest property/casualty insurance line, focuses on consumers so the approach is different compared to commercial lines such as general liability or business interruption coverage.

Further, the traditional insurance paradigm is evolving to a data and analytics model. Insurance executives, who tend to be conservative in nature, are still learning to maximize predictive modeling so it extends beyond underwriting and pricing to addresses claims management practices and marketing techniques. Forward-moving insurers are focusing on obtaining business intelligence through predictive modeling, which is quite difficult to understand without insurance expertise.

Other disruptors, including artificial intelligence, changing regulations and policy sales via Internet are also having a great impact on insurance companies and the vendors that serve them. Vendors that want to expand into the insurance industry also struggle with understanding what insurers really need, industry nomenclature or the right point person to contact.

Meanwhile, each insurance line faces its own struggles. Auto insurers see promise in telematics when many consumers want personal privacy. Then there are "preoccupiers" such as Uber and Lyft and driverless cars.

...the C-Suite commonly does not want to accept that publishing is expensive.

Then there is the problem of truly understanding the needs of each customer type. Insurers are vying for a greater piece of the growing demand for cyber coverage. However, policies are inconsistent. Buyers – and even their agents – are struggling to know what should be included in their coverage. The market potential for cyber insurance is enormous, but developing the right policy per each specific customer profile remains a challenge.

For business insurance, a smaller company that lacks a risk manager or a really awesome agent or broker will purchase based on price. Larger companies see the value of services and are

sophisticated enough to know that price is just one part of the equation. They want to know how an insurer's services will support risk management, claims processing and other areas. They also need to be sold on the technology. All of this requires expert insurance content.

Another limitation is that marketing companies often approach digital marketing from a business school rather than a journalism school approach. They lack professionals who understand how to effectively produce materials. They are not trained in first rule of journalism, which is to understand the audience. I often encounter companies that do not want to invest in determining customer needs and pain points. Without understanding the audience, expert insurance content for inbound marketing will fail.

So what is the solution? Check out Part 2 of Facing the Insurance Quality Content Dilemma.

In the meantime, please offer your comments below or drop me a line at annmarie@insurancecommunicators.com.

The Actuarial Cyber Coverage Conundrum

http://www.actuarialreview-digital.org/

Are insurance companies offering cyber coverage collecting enough money to cover future cyber events?

Nobody really knows, but there is reason for concern.

Insurance companies are offering more cyber coverage to gain market share. At the same time, data hackers too often elude cyber security experts. In fact, the amount of cyber incidents, including data breaches, continue to climb just as insurers fear a cyber hurricane that could wipe out major systems practically at the same time.

These are just some of the topics covered in my article, *"Cyber Insurance: The Actuarial Conundrum,"* which was published today in Actuarial Review, the magazine of the Casualty Actuarial Society.

My article defines the conundrum that actuaries face and also examines topics that should interest the non-actuary including the insurance market and the challenges of cyber security.

Here's the conundrum: how can actuaries appropriately price ever-changing cyber risk when data is scarce and models remain under development?

Besides digging into the conundrum's implications, my article also offers ways actuaries can, as they do with other insurance lines, get more deeply involved in the underwriting process. The article also offers alternative ways actuaries can gain potentially relevant data and develop models.

I hope you find the piece to be both enlightening and helpful.

To read my other articles on cyber insurance, click here.

Cyber Coverage and the Actuarial Challenge

http://www.contingenciesonline.com/contingenciesonline/20150102#pg46

Major cyber attacks are almost becoming the flavor of the month. Sony, JP Morgan, the Home Depot, the U.S. Postal Service, the Target Corporation — the list goes on and on.

If there is anything more challenging than preventing cyber attacks, it is figuring out how to cover the growing risk.

As I cover in my recently released *Contingencies* article, ***"Plugging Data Security Breaches,"*** underwriting is especially difficult. Since the cyber insurance market is growing exponentially, carriers are eager to snap up market share. Meanwhile, their actuaries are concerned about

carrying greater liability and pricing.

When it comes to pricing, like any emerging type of insurance, lack of historical data is a big actuarial challenge. Without historical data, actuaries cannot drive using the rear view mirror. Unfortunately, at some point, it seems there will be enough cyber breaches to address that challenge.

At the same time, actuaries will need to use future-forward data and assumptions to prepare for the unimaginable. As I cover in an ***Actuarial Review*** article, these challenges are similar for actuaries dealing with terrorism coverage. Because cyber risks and attacks are becoming more serious and hard to anticipate, I predict that the federal government will eventually offer a backstop for cyber insurance just like for terrorism coverage. Technological innovations, as outlined in **a previous *Contingencies*** article, will help actuaries rise to these challenges.

Without historical data, actuaries cannot drive using the rear view mirror.

The good news is that insurers are getting smarter on how they offer cyber coverage and pricing. To even procure cyber coverage, customers must demonstrate meaningful and defined risk management strategies. I predict that insurers will require even more risk management as best practices continue to emerge.

Cyber Terrorism Threat Continues to Emerge

As for predicting the unimaginable, cyber attacks are also rising to the level of acts of terrorism. A year ago when the Target breach was making headlines, companies were concerned about facing the liabilities for cyber attacks that usually went after the personal and financial information of their companies and customers.

The recent cyber attack on Sony however, is a different animal when hackers threaten violence at movie theaters that show a particular film. This is especially true if the CIA is right and the attack came from the North Korean government. Even if the current theory, that former Sony employees were behind the attack, is correct, this new way of threatening businesses and individuals is likely to be another factor actuaries will need to consider when pricing coverage.

The truth is, nobody knows what is next. While my new article also talks about a Cybergeddon that could cripple the U.S. economy or even worldwide, there is also grave concern that attackers will destroy utility computer systems, which has repercussions too terrible to imagine.

If the past is the best predictor of the future, I have full faith that actuaries will work through their challenges. After all, they are not just number crunchers, but creative thinkers who can use technology to its best advantage.