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.

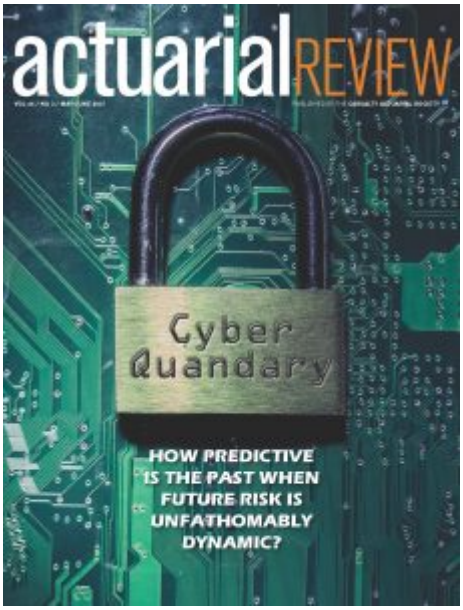
The bad guys,
who have the creativity to walk
the gauntlet of cyber protections,
are quite innovative.

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.

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.

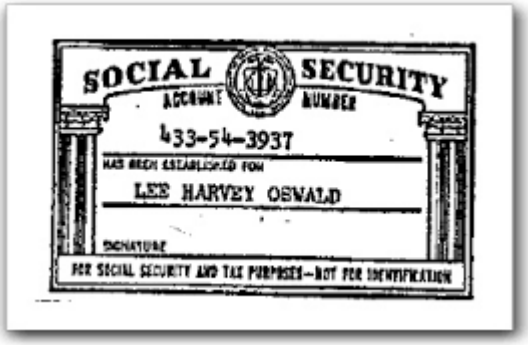
To read my other cyber insurance articles, please click here.

Data Breach Vulnerability Not Just Due to Technology

About 21.5 Americans' social security numbers and other sensitive personal information were compromised due to the hack of the U.S. Office of Personnel Management, according to an article posted today on cnn.com.

It seems data breaches have become so common that those unaffected are undocumented workers or Amish.

How did personally identifiable information become so vulnerable? The answer isn't limited to the technology.



Social Security Administration (public domain) via Wikimedia Commons

Our vulnerability is actually the result of a combination of historical, social and economic factors. To improve protection of personal information, it is important to consider how we got here.

A Little History

Before social security numbers were assigned to Americans, identity was simply a person's name. After spending decades on genealogical research, I can attest to the fact that before the 1900 census, the government asked very little personal information about Americans.

When President Franklin Delano Roosevelt began the Social Security program as a response to the Great Depression, social security numbers were only to be used for the program. Old social security cards indicate that the numbers are "not for identification." Just check out the Social Security card of Lee Harvey Oswald, who purportedly assassinated President John Fitzgerald Kennedy.

Over time, corporations got away with using social security numbers as identification for multiple purposes. It's been necessary for obtaining credit or health insurance purposes since at least the mid 1980s. When I started college in 1986, my identity number was my social security number.

I suspect that cell phone numbers will also become a necessary form of identification that will evolve into being used on a "mandatory" basis just like social security cards.

A Generational Divide

Socially, the culture of the United States has changed from one of valuing personal privacy to one of perpetual sharing. "It ain't none of your business," was a very common retort when I was growing up.

The vulnerability of Americans' personal information is not just due to technology getting ahead of us, but also to changing values of privacy.

Millennials and younger are less likely to believe privacy is a big deal. This group most fully embraces social media and "sharing" – including Too Much Information (TMI) sharing that was once considered socially impolite. The ramifications of Facebook's privacy policy might also surprise them. And honestly, I don't think the younger generations care even though nobody really knows who is "listening."

For Americans to begin caring about personal privacy again, enough might have to suffer the consequences of losing (or even sharing) private information. For example, if you knew anyone who suffered through the Great Depression, you might have observed how that generation saved everything "just in case." Because of the great suffering, Roosevelt got the support necessary to start social security.

But for now, Americans seem more engrossed in Caitlyn Jenner and gender identity issues rather than the ultimate identity issue: someone stealing yours and using it for criminal activity, extortion or even terrorism.

Some of this theft comes from information Americans willingly share on the Internet. Other important data, including financial and medical information, is being breached from the government and corporations. Combine that public information once stored on paper files and the opportunities for harm are endless.

We have already seen ISIS threaten individual military members and their families because Facebook can give a clue to their home and Google Maps will point the way there. Terrorists can certainly do the same to civilians as well.

As a Gen Exer, I was most influenced by the Baby Boomers. They were my younger professors who taught me women's studies, gay politics and civil liberties. They all stressed that American freedom includes the universal right to privacy for all Americans.

Baby boomer President William Jefferson Clinton, along with Congress, thought protecting personally identifiable health information was a big deal. He was instrumental in passing through the Health Insurance Portability and Accountability Act (HIPAA). (Interestingly, workers' compensation was excluded from the Act.)

For the majority of Americans, HIPAA is now just part of the pile of papers they need to sign at the doctor's office. The law was enacted before the rise of Internet commerce and when Baby Boomers and older generations were the majority of the country. Complying with HIPAA only gets ting more difficult as paper medical records are being converted to electronic files.

Then Gen Exer President Barack Obama ushered in the Affordable Care Act, which throws medical privacy out the window. Now the federal government has access to your medical records because health insurers and medical providers are required to share them.

For Americans to begin caring about personal privacy again, enough might have to suffer the consequences of losing (or even sharing) private information.

Federal agencies are hardly safe custodians. Just ask the potential 9+ million past and present federal workers and our military whose data is now vulnerable to whoever hacked it.

Further, cyber incidents, including data breaches, are on the rise according to Verizon's "2015 Data Breach Investigations Report." Add to that 66 percent of accountable care organizations surveyed last year by the Ponemon Institute, who believe patient privacy risk has grown and do not have great faith in data security.

Conclusion

The vulnerability of Americans' personal information is not only just due to technology getting ahead of us, but also to changing values of privacy. Looking back to history and considering past policy and social mores provides context for developing ways to promote privacy. I have a few ideas in mind and soon I will share them in a future blog.

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.

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.

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 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.