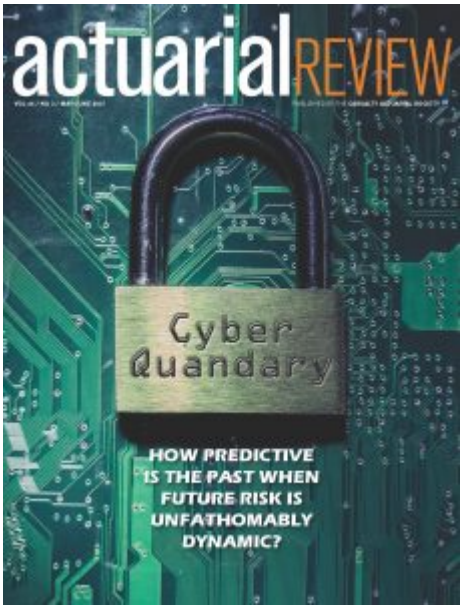
New Developments in Cyber Insurance Address Growing Needs



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.