ALLIED WORLD'S GLASGOW ADVISES CLOSE EYE *on* CYBER REGULATORY ENVIRONMENT

Advisen executive interview: Jason Glasgow, Allied World

By: Erin Ayers, Advisen

The cyber insurance market continues to evolve amid ever-changing threats and regulatory developments, and Jason W. Glasgow, recently appointed head of Allied World's privacy and network security group, said the insurance industry is working to meet the challenges of a changing environment.

In a recent interview with Advisen, Glasgow discussed the expansion of interest from insureds in many different industries and the increased awareness of cyber risk.

"The good news is that organizations are more aware of it," he said. "It used to be seen as a risk for retailers; now more and more companies realize they can be affected. Brokers have done a tremendous job educating their clients."

For its part, the insurance industry is honing its ability to underwrite a complex risk that is affected significantly by not only the regulatory and legal landscape, but also the controls that organizations put in place to reduce security breaches. Glasgow spoke about Allied World's 10 years in the cyber insurance market and his new team's "nimble, creative" approach to keep pace with the changing environment.

"WE'VE BECOME MUCH MORE SOPHISTICATED IN LOOKING AT THOSE CONTROLS AND EVALUATING BASED ON THOSE CONTROLS."

"Cyber encompasses a number of different dynamic risks," said Glasgow. "We've become much more sophisticated in looking at those controls and evaluating based on those controls."

Glasgow emphasized the resources available to businesses looking to understand and mitigate their cyber risk.

"The government has sponsored 18 different information sharing and analysis centers, ISACs. I always encourage businesses to join," said Glasgow. "That level of cooperative communication is essential."

With the globalization of cybercrime, organizations have even more of an imperative to arm themselves with technology, information, and insurance.

"Fifteen years ago, hackers were operating out of their basements. Now, they're much more organized, working to try and find money or information they can monetize," he said.

He added that as regulators evaluate cyber guidelines for the industries they oversee, businesses should be aware of the potential impacts.

"The regulatory environment has really driven the cyber market. As exposures continue to evolve and litigation ensues, what are guidelines now will become legal standards," said Glasgow. "There's some grey area there now."

Cybercriminals operate in waves, taking advantage of vulnerable businesses. Glasgow explained that a few years ago,

"HAVING INSURANCE AGAINST THESE TYPES OF RISKS IS CRITICAL"

the retail environment was particularly vulnerable and criminals were able to easily monetize credit card information. The retailers got smarter, improved their cybersecurity posture. Criminals, however, will continue to develop new ways to attack retailers and are expanding their targets, such as the healthcare sector.

"Now it's small and mid-sized businesses," said Glasgow. "We're seeing malware getting on the systems of smaller businesses, causing transfers of money and information. These kinds of smaller-scale attacks are happening all the time."

Greater awareness is needed among those businesses that feel they aren't at risk, he added.

"I can tell you from claims history that it does happen every day. It costs them real dollars. Having insurance against these types of risks is critical," Glasgow said.

He advises brokers and insureds to seek out established cyber markets with "robust" risk management services and pre-breach assistance.

"When looking at carriers, look at how they help their insureds," said Glasgow. "Is it merely a portal of information that can be found on the internet, or will the insurer truly provide tailored and hands-on support to help protect an organization?"

The "next wave of regulation" for organizations to navigate will focus on an increasingly connected world of technology – drones, smart homes, and driverless cars, to name a few. Keeping a sharp eye on the industry standards and breach notification requirements in all US states will be a must for all in the insurance industry.

"There are 47 different reporting requirement statutes," said Glasgow. "Businesses often need expert help navigating those ocean waters."

Offering a few words of advice to brokers and businesses, Glasgow emphasized planning for the future.

"HAVING A PLAN IN PLACE AND BEING ABLE TO RESPOND QUICKLY AND MITIGATE THE LOSSES WHEN THEY HAPPEN IS OFTEN MORE IMPORTANT THAN THE TECHNOLOGY."

"I often tell businesses that are taking a look at a cyber application, if they're answering no on the questions for insurance, regardless of whether they buy insurance, they should be looking at their preparation," he said. "Having a plan in place and being able to respond quickly and mitigate the losses when they happen is often more important than the technology."