[INSIGHT] By Peter H. Bickford

Cyber Insecurity

Although insurance industry players – companies and producers – are not exactly modern Luddites opposed to any technology advances, it is no secret that the industry usually lags behind in keeping up with an ever-changing world. In an age where young people in the same room are more comfortable communicating via texting rather than talking to each other, the business of insurance clings to personal interface as a keystone. Some consider this a strength of the industry while others seem to always be pushing the industry to wider, more dynamic acceptance of modern technology to keep pace or risk losing its position in the world economy. It should be no surprise, therefore, that the industry is being pressed to recognize and protect itself and its customers from cyber threats. When that pressure comes from regulators – themselves technology challenged – it should raise a few eyebrows!

Peter H. Bickford

Of all the "hot topics" in the world of insurance regulation, the current regulatory frenzy over cyber security is right up there with excessive financial standards and SIFI (Systematically Important Financial Institutions) designations.

Of all the "hot topics" in the world of insurance regulation, the current regulatory frenzy over cyber security is right up there with excessive financial standards and SIFI (Systematically Important Financial Institutions) designations. Every regulatory level is in on the act, from the Federal Insurance Office (FIO), to the National Association of Insurance Commissioners (NAIC), to individual states like the New York Department of Financial Services (DFS).

The most aggressive, of course, is New York's DFS, whose chief has repeatedly stated that cyber security is the primary regulatory topic of concern for the foreseeable future. To back up this concern, the DFS produced a report in February on Cyber Security in the Insurance Sector after having produced a similar report on Banking Cyber Security last spring. The insurance sector report, based on surveys conducted even before the Anthem security breach was publicly disclosed, concluded that outside of their IT units most company managements had minimal knowledge of the scope and seriousness of the problems relating to securing information or how to address these problems.

These findings prompted the DFS to issue a letter to licensed insurers in March advising them that the Department "intends to schedule IT/cyber security examinations after conducting a comprehensive risk assessment of each institution." To aid in that assessment, the Department "requested" a report from each insurer to be submitted by the end of April addressing 16 specific areas of inquiry regarding its security platform and standards.

At the other end of the spectrum, of course, is the NAIC, which at its spring meeting adopted "Principles for Effective Cybersecurity: Insurance Regulatory Guidance" as recommended by its cybersecurity taskforce. The NAIC document includes 12 broad principles addressed not just to insurance companies, producers and other licensees but also includes principles aimed at regulators and their obligations (the NY letter and its 16 specific areas of inquiry are addressed only to insurers). The NAIC cybersecurity taskforce acknowledged that its principles were derived from a similar earlier effort by the securities industry.

The NAIC guidelines as approved made two changes from the initial draft to address industry criticism. First, the language was softened to address concerns that the original draft guidelines were too inflexible or too closely skewed to a specific standard. The other change was to remove a number of guidelines relating to the sale of cyber risk insurance. However, where the New York framework is devoid of reference to cyber insurance products, the NAIC Cybersecurity Taskforce, in addition to its guidelines, is considering a comprehensive, mandatory annual supplement detailing insurers' cybersecurity policy writings to help regulators understand the size, scope and activities of the market. The NAIC is also working with Federal regulators and the FIO to coordinate data collection efforts on the scope of the marketplace for cyber risks.

Which brings us to the FIO and its announced plans that seem to go beyond the collection of data on cyber risk writings into the world of establishing underwriting guidelines for these risks. Huh? Regulators establishing underwriting guidelines?

In discussions among regulators, there has been much chatter about the need to coordinate the collection of cyber security data. There also seems to be regulatory recognition that increasing access to cyber coverage can be a significant mitigating factor in cyber crimes by making businesses incorporate better risk management systems. Recognizing underwriters' need for incident frequency and severity data on cyber risks, however, does not ensure that this data will be successfully collected or made available to underwriters anytime soon. There are still substantial hurdles to be overcome in order to make this happen including the confidential nature of much of the data, National security concerns and the reluctance of targets to be fully open about breaches of their systems. Nobody

continued on page 8

continued from page 6

wants its system vulnerabilities on public display.

It seems a bit premature, therefore, for the FIO to leap from unresolved data collection and availability issues to the realm of insurance underwriting, not to mention the incongruity of government establishing underwriting standards for private businesses. It may be that when the FIO suggests establishing underwriting guidelines for cyber risks it has in mind things like defining acceptable minimum coverages, or identifying public policy consideration – items that permeate state insurance laws in areas like homeowners, auto and health insurance coverages. But who knows? Like financial standards being determined in large part by bank-centric regulators, the insurance industry - pushed again to the periphery of the dialogue - hopes that its limited voice on cyber security is loud enough to be heard and considered.

And who understands New York? While the NAIC and the FIO at least evidence some understanding of the positive relationship between expanding the cyber risk marketplace and risk mitigation, New York seems singularly focused on insurers' own internal systems and protections. The few references to expanding cyber risk markets are incidental to the extensive and detailed directives to the companies about their own internal controls.

Like financial standards being determined in large part by bank-centric regulators, the insurance industry - pushed again to the periphery of the dialogue - hopes that its limited voice on cyber security is loud enough to be heard and considered.

I suppose I should not be surprised at yet another example of New York's reluctance to actually support growth and expansion of the business of insurance in the state. However, in view of the multiple pronouncements by New York's chief banking and insurance regulator on the primacy of cyber security as a regulatory concern for the foreseeable future, wouldn't it behoove the state to be more enthusiastic in expanding the market for cyber insurance products?[IA]

Peter Bickford has over four decades of experience in the insurance and reinsurance business, with particular focus on regulatory, solvency, agency, alternative market and dispute resolution issues. In addition to his experience as a practicing attorney, he has been an executive officer of both a life insurance company and of a property/casualty insurance and reinsurance facility. A complete biography for Mr. Bickford may be accessed at www.pbnylaw.com.