Insurance Times: Conning: Insurers facing considerable cyber-security exposure
November 13, 2001, Vol. XX No. 23

HARTFORD — The somewhat laggard entry of many insurers into online' distribution of policies and services now may be exposing their customers, business partners and themselves to massive losses caused by breaches in security, according to a new study from the insurance investment and research firm, Conning & Co.

The Conning study, Cyber-Security for Insurers: The Virtual Fortress?, explains that insurers may be very attractive targets for attacks. First, insurers manage substantial liquid financial assets of their own as well as others'. Second, they may be specifically targeted by aggrieved hackers to avenge perceived ill treatment. Finally, insurers may be considered by some to be relatively easy targets because of their heavy reliance on “legacy" computer systems, relatively recent ventures into Internet-based processes, and growing interconnectivity with a large number of business partners. Structural changes associated with mergers and acquisitions and recent “downsizing" also may increase insurers' security vulnerabilities.

“It is critical that insurers address their cyber-security vulnerabilities because of the substantial costs associated with breaches and the serious reputational damage that could result," warned Clint Harris, vice president at Conning and author of the study. “The trends are ominous for all industries," he continued.

Losses associated with cyber-security breaches, as we defined in the study, are projected to increase to $46.3 billion by 2005, more than twice the amount as in 2000.

Even this considerable cost likely underestimates potential losses because it does not include so-called “soft costs", such as degradation of brand image.

In addition to holding important “information assets", insurers maintain highly sensitive, personal information such as medical records.

“What is the cost of having a person's life devastated because sensitive information was stolen and publicized? The monetary settlement cannot replace the trust insurers have built with their customers and business partners," said Harris.

The study maintains that the proliferation of rules, regulations and standards regarding cyber-security is more likely to escalate than abate in the near future. However, too great a focus on the security-related privacy provisions of the Gramm-Leach-Bliley Act of 1999 (GLBA) or the Health Insurance Portability and Accountability Act of 1996 (HIPAA) may actually result in reduced security. The difficulty in concentrating on complying to external standards is that those standards can be ambiguous, subject to change and may actually distract the company from its true internal cyber-security objectives.

“In conducting this study, we discovered that some insurers may be in denial about their cyber-security risks," said Harris. “Their argument is ‘We haven't had a major incident so there's no reason to panic. We spent millions on Y2K, perhaps unnecessarily, and we have no intention of repeating that.’ Insurers need to recognize that systems vulnerability is a very different exposure than the Y2K bug. First, there are large losses resulting from breaches already. Second, unlike Y2K, there is no end date for the exposure. Finally, cyber-security exposures are projected to escalate due to insurers' increased reliance on more open technologies, growth and maturity of cyber-security attackers, and structural changes that continue to change the industry."

The study is available at the company's Web site at www.conning.com.