Published on *The National Law Review* https://natlawreview.com

IAIS Secretary General Considers Path to International Cybersecurity Standard

Article By:

J.J. Silverstein

Last week, the National Association of Insurance Commissioners (NAIC) hosted the 2016 NAIC International Insurance Forum. The Forum addressed topics such as the management of catastrophic disaster risks, industry perspectives on international insurance standards, and cybersecurity and cyber insurance.

As part of the Forum, Adam Hamm, commissioner of insurance for North Dakota and the NAIC Cybersecurity Task Force's chair, moderated a panel discussion on cybersecurity and cyber insurance. Dr. Yoshihiro Kawai, the International Association of Insurance Supervisors (IAIS) secretary general was asked during that panel whether cybersecurity was an issue that could be addressed through a system of internationally harmonized regulations. In response, Dr. Kawai stated that the IAIS was addressing this issue with a step-by-step process. The first step, he noted, was the collection of information from supervisors and industry participants worldwide to determine the current state of cybersecurity practices and regulation. He added that this step was a learning process for the IAIS, but that once it is complete, the IAIS will be able to move toward creating a global cybersecurity standard based on that information.

If that process comes to fruition, it may be in the form of a new IAIS Insurance Core Principle on cybersecurity. Insurance Core Principles (ICPs) are components of the IAIS's internationally recognized framework for regulation of the insurance industry. Though a cybersecurity ICP would not constitute legally binding authority over insurance commissioners in the United States or supervisors in other countries, the ICPs are used in assessments of insurance supervisors by the World Bank and International Monetary Fund. A new cybersecurity ICP, or the incorporation of cybersecurity principles into existing ICPs, would therefore create an influential minimum expectation for regulation of the insurance sector's cybersecurity practices.

The IAIS notes, in its recent *Issues Paper on Cyber Risk in the Insurance Sector*, that many of its ICPs provide "a general basis for supervisors to address the insurance sector with respect to cyber risk and cyber resilience." These include ICPs relating to corporate governance (ICP 7), risk management and internal controls (ICP 8), information exchange and confidentiality requirements (ICP 3), and others. It is possible that the IAIS could merely revise one of these related ICPs to

address cybersecurity. According to the report, “the [IAIS Financial Crime Task Force] will be investigating whether — and if so, how — ICP 21 [on countering fraud in insurance] should be extended to specifically address elements of cybersecurity.” That approach would be similar to the one originally contemplated by the NAIC, whereby the Insurance Information and Privacy Protection Model Act and the Privacy of Consumer Financial and Health Information Regulation would have been revised to address their cybersecurity concerns. However, given Dr. Kawai’s statements at the Forum, and the NAIC’s decision to address these issues in a separate Data Security Model Law, it is also possible that the IAIS will explore the creation of an entirely new ICP on cybersecurity.

If so, the IAIS would likely draw on two major sources in drafting a cybersecurity ICP: (i) the information gathered in drafting the IAIS *Issues Paper on Cyber Risk to the Insurance Sector* (along with the comments the IAIS is currently reviewing in response to the *Issues Paper*) and (ii) the NAIC Data Security Model Law (a draft of which is under discussion by the NAIC’s Cybersecurity Task Force, and will likely be finalized over the next six months). Given the issues addressed in these documents, it is likely that a cybersecurity ICP would include requirements such as ensuring that:

- Supervisors have a thorough and comprehensive understanding of the cyber threats to the insurance sector;
- Supervisors have an effective framework to monitor and enforce compliance with regulations that counter cyber threats ; and
- Supervisors have effective mechanisms to coordinate with other supervisory authorities regarding cyber threats.

Most important, a cybersecurity ICP would likely include a requirement that supervisors adequately address cyber threats through legislation and guidance. In its *Issues Paper*, the IAIS highlighted numerous cyber threats to the insurance industry. The extent to which a cybersecurity ICP would specifically address these risks and require implementation of legislation requiring particular data security procedures, data breach notification requirements, and data breach remediation requirements by insurance licensees is unknown. A softer approach would be to require supervisors to address cyber threats through “adequate” legislation and/or guidance on these subjects. However, if the IAIS intends to address these nuanced data security issues, it would not wish to rely on broad standards for the implementation of legislation. What is “adequate” or “sufficient” in the context of cybersecurity remains unclear and is constantly evolving.

The IAIS highlighted three “Examples of Cybersecurity Weaknesses” in its *Issues Paper*, including “Missing or Incomplete Overview of the IT-Landscape,” “Inadequate Control Process Regarding User Privileges,” and “Improper Access to Superuser Accounts.” To address these and other specific issues of data security, the IAIS may choose to adopt the NAIC’s more detailed approach. The current draft of the NAIC Data Security Model Law attempts to address similar weaknesses by requiring insurers to have a comprehensive “Information Security Program” that is both “appropriate to” the “size and complexity” of the insurer and is benchmarked to the National Institute of Standards and Technology’s (NIST) framework on cybersecurity, including specific requirements as to encryption, multi-factor authentication, regular testing and monitoring, and restriction to physical locations where data is stored. However, requiring supervisors to implement such extensive rulemaking in a relatively recent and still developing area of regulation may be too much too fast.

A compromise between these two approaches would be an ICP that provides a list of areas that

legislation and/or guidance should address and ties the “adequacy” of the regulations related to these areas to standards set and maintained by other international organizations specifically focused on cybersecurity measures. This would allow supervisors the flexibility to implement rules tailored to their jurisdictions, while also spurring them to address topics constituting the most serious cyber threats.

Given that the IAIS is still reviewing comments submitted in response to its *Issues Paper*, and the NAIC is still in the process of revising its draft Data Security Model Law, it seems unlikely that a cybersecurity ICP would be issued this year. However, as part of the increased international coordination and conversation among supervisors on cybersecurity issues, a new cybersecurity ICP or the amendment of existing ICPs to address cybersecurity concerns appears likely. Therefore, insurers and insurance-related entities with multinational regulatory exposure should keep an eye on the expansion and evolution of these benchmarking standards.

National Law Review, Volume VI, Number 148