A little over one year after the National Institute of Standards and Technology (NIST) issued its Framework for Improving Critical Infrastructure Cybersecurity, the National Association of Insurance Commissioners (NAIC) – the national regulatory support organization for insurers – has issued 12 guiding principles to promote enhanced security.

The NAIC took this step in response to a couple of prodigious data breaches at two large health insurers. The first reported in early February that hackers had obtained information of over 80 million of its customers, roughly double the amount of records affected during a large retailer’s high profile data breach last year. The company subsequently announced that breached information included names, birthdays, Social Security numbers, health care ID numbers, home addresses, email address and employment information – but not payment card data or medical information.

Then, on March 17, the second insurer disclosed that it too had suffered a data breach involving approximately 11 million customer records. Importantly, it appears that this insurer’s breach likely exposed sensitive information, such as bank account numbers and clinical information.

Both cyber incidents highlight the immense challenges presented to health insurers in defending themselves from sophisticated and targeted cyber-attacks.

WHO IS IMPACTED?

The SEC guidance (released November 2011) and NIST framework (released February 2014) apply to publicly traded companies and critical infrastructure, respectively. Meanwhile, the NAIC serves as the national system of state-based insurance regulation in the United States, so the 12 guiding principles pertain explicitly to organizations operating in the insurance industry. Clearly, the NAIC has been compelled to weigh in as they attempt to shelter their industry through a tempest that appears to have no end in sight.
THE TWELVE GUIDING PRINCIPLES

1. State insurance regulators should collaborate with insurers, insurance producers and the federal government to achieve a consistent, coordinated approach to information security.

2. Confidential and sensitive information stored outside of an organization’s computer systems should be appropriately safeguarded.

3. State insurance regulators have a responsibility to protect information that is collected, stored and transferred inside or outside of an insurance department or at the NAIC. In the event of a breach, those affected should be alerted in a timely manner.

4. Cybersecurity regulatory guidance for insurers and insurance producers must be consistent with nationally recognized efforts, such as those embodied in the NIST framework.

5. A minimum set of cybersecurity standards must be in place for organizations operating in the insurance industry.

6. State insurance regulators should provide appropriate regulatory oversight and conduct risk-based financial examinations and/or market conduct examinations regarding cybersecurity.

7. Planning for incident response is an essential component to an effective cybersecurity program.

8. Appropriate steps should be taken to ensure that third parties and service providers have controls in place to protect personally identifiable information.

9. Cybersecurity risks should be incorporated and addressed as part of an organization’s enterprise risk management (ERM) process.

10. Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurer’s board of directors.

11. It is essential for organizations to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.

12. Periodic and timely cyber security training, paired with an assessment, is essential.

IMPLICATIONS FOR HEALTH INSURERS

These guiding principles lay good groundwork, effectively outlining areas of focus for state regulators. However, several principles (e.g., principles 2, 6, 8) do not expand in sufficient detail on specific action items regulators should be imposing on insurers. For example, what benchmark defines third-party information as “appropriately safeguarded?” Principles 6 and 8 encourage regulators to focus heavily on oversight, without imposing specific requirements on state entities. It appears that the SEC guidance may have paved an avenue for shareholder litigation arising from inadequate management or disclosure of cyber risks. Will these guiding principles help foster future privacy actions against organizations or state regulators (for failure to manage industry risk)? Only time will tell.

Ultimately, as was the case with the SEC guidance and NIST framework, the guiding principles issued by NAIC do not constitute formal regulatory requirements. Rather, the NAIC appears to have been encouraging state regulators to be more active and assist in the adoption of uniform standards in an area where risk management is struggling to keep pace with the tactics employed by the most organized cyber criminals.

In addition to considering and implementing these guidelines where feasible and appropriate, organizations operating in the insurance industry should also consider the involvement of risk advisers that can:

- Collaborate effectively with regulators, the federal government and insurers to help formulate an effective strategy towards protecting consumer information
- Provide meaningful assurance that sensitive information in their custody or control is appropriately protected
- Play an important role in assisting their clients with preparing and implementing incident response
- Act as a capable adviser on effective compensating controls
- Be actively engaged in the enterprise risk management process, to effectively measure the likelihood and potential severity of a catastrophic cyber event
- Provide ongoing training and offer valuable insight into current and emerging industry threats

HOW WILLIS CAN HELP
Through our proprietary and world-class risk assessment tools including PRISM II℠, our experienced team of Cyber risk brokers will work with your organization to identify your cyber risk, evaluate and stress test your current risk management programs, review your third-party vendor contracts, and design an insurance program that is suitable for your organization based on your specific risk retention and risk transfer philosophy.


For additional information, please contact your Willis Client Advocate® or FINEX_NA@WILLIS.COM.

For past issues of our publications on other topics of interest, please visit the Executive Risks website.

FINEX Alerts and Newsletters provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advice in any specific situation.

Willis North America Inc.
Brookfield Place
200 Liberty Street, 7th Floor
New York, New York 10281-1003
United States
Tel: +1 212 915 8888

www.willis.com