Insurance Alert

NYDFS Calls for Insurers' Cyber Security Information by April 27

April 10, 2015

Follow us on

On March 26, the Superintendent of the New York Department of Financial Services (NYDFS) issued a letter detailing requirements for insurers to provide information related to their cybersecurity programs and practices. Due April 27, the short response time has created a sense of urgency among insurers.

In recent years, cyber security in the insurance industry has been a point of heightened concern for regulators. This latest initiative is a direct response to the many destructive breaches that have occurred in the United States financial system.

The reports, which are to be submitted via the NYDFS secure portal should contain responses to the following questions:

1. Provide the curriculum vitae and job description of the current Chief Information Security Officer or the individual otherwise responsible for information security, describe that individual's information security training and experience, and identify all reporting lines for that individual, including all committees and managers. In addition, provide an organization chart for your institution's IT and information security functions;

2. Describe the extent to which your institution maintains information security policies and procedures designed to address the information security goals of confidentiality, integrity, and availability. Provide copies of all such information security policies;

3. Describe how data classification is integrated into information risk management policies and procedures;

4. Describe your institution's vulnerability management program as applicable to servers, networks, endpoints, mobile devices, network devices, systems, and applications;

5. Describe your institution's patch management program, including how updates, patches, and fixes are obtained and disseminated, whether processes are manual or automated, and how often they occur;

6. Describe identity and access management systems employed by your institution for both internal and external users, including all administrative, logical, and physical controls and whether such controls are preventive, detective, or corrective in nature;

7. Identify and describe the current use of multi-factor authentication for any networks, systems, programs, or applications;

8. Describe all application development standards used by your institution, including the use of a secure software development life cycle, and the extent to which security and privacy requirements are assessed and incorporated into the initial phases of the application development process;

9. Provide a copy of, to the extent it exists in writing, or otherwise describe, your institution's incident response program, including how incidents are reported, escalated, and remediated;

10. Describe the extent to which information security is incorporated into your institution's business continuity and disaster recovery plan, the way in which that plan is tested, how often the plan is tested, and the results of the most recent test;

11. Describe any significant changes to your institution's IT portfolio over the last 24 months resulting from mergers, consolidations, acquisitions, or the addition of new business lines;

12. Describe your institution's due diligence process regarding information security practices that is used in vetting, selecting, and monitoring third-party service providers;

13. Provide a copy of any policies and procedures governing relationships with third-party service providers that address information security risks, including setting minimum information security practices or requiring representations and warranties concerning information security;

14. Describe any steps your institution has taken to adhere to the Framework for Improving Critical Infrastructure Cybersecurity issued by the National Institute of Standards and Technology ("NIST") on February 12, 2014 concerning third-party stakeholders;

15. Describe any protections that your institution uses to safeguard sensitive data that is sent to, received from, or accessible to third-party service providers, such as encryption or multi-factor authentication; and

16. List any and all protections against loss or damage incurred by your institution as a result of an information security failure by a third-party service provider, including any relevant insurance coverage.

Insurance companies authorized to sell policies in New York State that have been contacted are required to submit a report responding to all NYDFS requirements in a timely manner. If your company has not been contacted, we recommend gathering this information as a best practice.

How WeiserMazars Can Help

WeiserMazars is a leader in the Insurance and Information Security sectors. We have significant expertise helping clients compile this type of information. Our team of experts can significantly reduce the burden on your organization, ensuring that you are able to fully respond to the NYDFS, as well as provided insight into best practices and tools that can add value to your company.

For more information contact:

Nicolas Quairel, CISSP, CISA, CRISC
Principal, Information Technology Group
PH: 646.225.5983
Nicolas.Quairel@WeiserMazars.com

Vincent R. Burke, CPA
Partner
PH: 267.532.4308
Vincent.Burke@WeiserMazars.com

Visit us on **www.weisermazars.com**