OLD REPUBLIC NATIONAL TITLE INSURANCE COMPANY

Robyn E. Anderson
First Vice President, Chief Cybersecurity and Privacy Counsel
400 Second Avenue South, Minneapolis, MN 55401-2499 | T: 612.336-7062
randerson3@oldrepublictitle.com

December 13, 2018

Director Bruce R. Ramge, Chair
Market Conduct Examination Standards (D) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

Attn: Petra Wallace
Via e-mail pwallace@naic.org

Re: Insurance Data Security Pre-and Post-Breach Checklists

Dear Director Ramge,

We appreciate the opportunity to offer the following observations regarding the draft Pre-and Post-Breach Checklists (Checklists). It appears that the draft Checklists are intended to follow the requirements of the NAIC Data Security Model Law (Model Law).[1] Assuming that is the case, we offer the following observations to demonstrate where the Checklists appear to depart from the language of the Model Law which could create confusion and/or additional requirements beyond that of the Model Law:

1) Under Information Security Program (Sections 4A and 4B)
   a) Item number 2 asks, "Does the ISP clearly state the persons(s) at the licensee responsible for the program." There is nothing in Sections 4A or 4B that mentions this requirement. Section 4C(1) provides that pursuant to the risk assessment, "[t]he licensee shall designate one or more employees….who is responsible for the Information Security Program." There is a difference between these two requirements. A licensee may have designated responsible persons but not named those persons in the Company ISP documentation.
   b) Item number 3 asks, "Has the ISP been reviewed and approved by the Licensee's executive management?" There is nothing in Sections 4A or 4B that mentions this requirement. Section 4E(3) provides that "[I]f executive management delegates any of its responsibilities under section 4,…it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program

[1] The review guidelines and instructions provide "[w]hen reviewing a Licensee's Information Security Program for compliance with the Insurance Data Security Model Law (NAIC Model #668)…please refer to …[e]xamination checklists attached as Exhibit A [a]nd B hereto."

© 2018 National Association of Insurance Commissioners

prepared by the delegate(s) and shall receive a report from the delegates…" The difference here is the language "review and approve" versus "oversee".

c) Item number 4 asks, "Has the ISP been reviewed and approved by the Licensee's Board of Directors?" There is nothing in Sections 4A or 4B that mentions Board approval. In addition, Section 4E, which does address Board oversight, does not require review and approval of the ISP by the Licensee's Board of Directors. Rather, it provides that a committee of the Board shall "[r]equire the Licensee's executive management or its delegates to develop, implement, and maintain the Licensee's Information Security Program…"
d) Item number 5 asks, "Has the ISP been reviewed and approved by the Licensee's IT steering committee." We cannot find where there is such a requirement in the Model Law.
e) Items 10 and 12 appear to call for the same information regarding employee training. It is unclear if these requirements are intended to solicit different responses.
f) Item 13 appears to anticipate certain timing with regard to employee training but the Model Law provides only the following requirements, "[P]rovide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment (4)(d)(5) and, [A]ssess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including: (a) Employee training and management." (C)(4)(a). Neither of these requirements set a timetable for employee training.

2) Under Components of Information Security Program (section 4D)
   a) Item 19d states, "[S]ecure development practices for in-house applications and procedures for testing the security of externally developed applications." Section 4(D)(2)(e) of the Model Law provides the following language, "[p]rocedures for evaluating, assessing or testing." The deletion of the terms "evaluating" and "assessing" removes two of the three options available in the Model Law.

3) Under Incident Response Plan (section 4H)
   a) Item 30 introduces additional language and requirements into the Incident Response Plan regarding Third-Party Servicers that is not found in the Model Law section 4(H)(2)(a)-(g).
   b) Item 32 also appears to introduce additional language regarding "[v]arious levels of remediation based on the severity of identified weaknesses." This language is not found in 4(H)(2)(e).

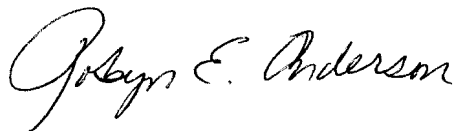
4) Under Documentation and Reporting Review Criteria
   a) Items 33 through 35 require certain documentation within the Licensee's ISP when it appears to be addressing requirements of 4(H) and therefore, requirements of documentation within the Licensee's Incident Response Plan.

© 2018 National Association of Insurance Commissioners

To be clear, we are not taking the position that the items in the Pre- and Post-Breach Checklists are unreasonable. We simply want to raise the issue that because the language used is different than the Model Law language there could be confusion and/or additional requirements imposed that go beyond the Model Law adopted by the NAIC.

We thank you for your consideration of these observations.

Sincerely,



Robyn E. Anderson
First Vice President, Chief Cybersecurity and Privacy Counsel

© 2018 National Association of Insurance Commissioners