Client Update
DFS Expands Its Cyber Focus to Insurers

NEW YORK
Eric R. Dinallo
edinallo@debevoise.com

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
David A. O'Neil
daoneil@debevoise.com

Jordan R. Friedland
jrfriedland@debevoise.com

On Thursday, March 26, New York State's Department of Financial Services (DFS) announced a major expansion of its cybersecurity efforts: DFS will require insurers to respond to a special "comprehensive risk assessment" on cybersecurity, with those assessments to be followed by an enhanced focus on cybersecurity as part of DFS's regular examinations of insurers. DFS's announcement expands to insurance the increasingly rigorous approach it has recently applied to banks in the area of cybersecurity. More importantly, it offers critical guidance to all industries about what regulators will consider adequate precautions and preparation in this area.

THE DFS LETTER

The DFS action took the form of a so-called "308 letter" from Benjamin Lawsky, the DFS Superintendent, to CEOs, general counsels and CIOs of insurers. Section 308 of the New York Insurance Law gives DFS broad information-gathering powers. This 308 letter spells out the details of the one-time comprehensive risk assessment in the form of a detailed written questionnaire that must be answered by April 27. Insurers will have to answer questions about a broad range of cybersecurity issues – many of which mirror those that DFS required banks to answer in December 2014 – including:

- Corporate governance of cybersecurity, including the curriculum vitae and job description of the Chief Information Security Officer or other senior person responsible for cybersecurity;
- Policies and procedures designed to further the goals of confidentiality, integrity and availability of data, including the integration of data classification (a/k/a the sorting of data according to its sensitivity and risk level) into such policies and procedures;

- Various highly specific security topics, such as the use of multi-factor authentication, patch management, penetration testing and vendor management. (N.B.: It is a matter of public record that criminals' abuse of credentials issued to third-party vendors has been implicated in a number of recent, high-profile hacks.);
- Steps 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;
- Policies and procedures governing relationships with third-party service providers that address information security risks;
- Protections used to safeguard sensitive data that is sent to, received from or accessible to third-party service providers, such as encryption or multi-factor authentication;
- Protections against loss or damage incurred as a result of an information security failure by a third-party service provider;
- Incident detection and response processes, including real-time monitoring and the institution's written incident response plan;
- Cyber insurance coverage; and
- Periodic reevaluation of policies and procedures in light of changing risks.

In the 308 letter, DFS notes its expectation that companies will make efforts to obtain any information necessary to respond to the questionnaire from parent or affiliate companies, and imposes upon parent companies the obligation to obtain such information from subsidiaries.

IMPLICATIONS FOR INSURERS AND OTHER COMPANIES

DFS has not promulgated specific cybersecurity standards, but it is strongly suggesting what it considers best practices by the questions it asks. We have previously called that "regulation by implication" – the questions themselves imply answers that the agency is likely to prefer. Strong substantive answers on the enumerated topics, clearly presented, can be expected to generate clean examination reports. Answers that DFS considers highly unsatisfactory, in contrast, could prompt DFS to pursue civil enforcement measures.

Take multi-factor authentication as an example. For the uninitiated, this is the practice of requiring more than a single username/password combination to access a computer system – for instance, use of a one-time code received via a

token or text message in addition to a password is a common form of multi-factor authentication. No state or federal law expressly dictates the use of multi-factor authentication, but by asking companies to describe their practices in this area, DFS is clearly signaling that, going forward, it hopes to see companies adopt policies and procedures favoring multi-factor authentication. That is consistent with Superintendent Lawsky's comments, in a February 25 speech, that DFS was considering promulgating regulations mandating the use of multi-factor authentication because, according to Lawsky, single-factor authentication "should have been dead and buried many years ago," and "it is time that we bury it now."

Another example is the new requirement (not previously applied by DFS to banks) for institutions to describe steps they have taken to adhere to the Cybersecurity Framework promulgated by NIST. The NIST Framework does not have the force of law, though DFS's reliance on it is yet another indication that the standard is increasingly seen as the emerging gold standard of cybersecurity benchmarks. Simply by asking about the NIST Framework, DFS nudges it toward preferred legal status. That being said, nothing in DFS's guidance suggests that alternative benchmarking tools like ISO or SANS are inadequate or flawed.

This approach of regulation-by-inquiry is reflected throughout the DFS guidance: Simply by asking pointed questions – about vendor management, patch management, the use of written incident response plans and so on – DFS is dropping strong hints as to what it will consider "right" answers in the context of the examinations it will conduct in 2015.

Although the most recent DFS guidance specifically applies only to the insurers it regulates, management and boards throughout corporate America would do well to study both this guidance and the guidance issued to banks in December 2014. Companies that suffer cybersecurity incidents increasingly are facing pressure to defend themselves – whether in private litigation or in regulatory enforcement actions. Companies in all industries thus may find the DFS "308 letter" a useful checklist for assessing their own cybersecurity posture.

* * *

Please do not hesitate to contact us with any questions.