Data Governance Requirements to Support Compliance with New York State's Cybersecurity Regulation

by Sunil Soares
July 27, 2017

The New York State Department of Financial Services recently released 23 NYCRR 500, a regulation dealing with Cybersecurity Requirements for Financial Services Companies. The regulation went into effect on March 1, 2017, and covers entities that are regulated by New York State's Banking Law, Insurance Law, and Financial Services Law. The regulation places a number of requirements on covered entities, including the following:

- Maintenance of a cybersecurity program
- Implementation and maintenance of a written cybersecurity policy
- Designation of a chief information security officer
- Penetration testing and vulnerability assessments
- Risk assessments
- Training and monitoring
- Encryption of nonpublic information
- Responses to incidents such as data breaches
- Annual attestation regarding compliance with the regulation

Many of these requirements are likely part of existing cybersecurity programs at financial services companies. However, data governance programs can also support compliance with this regulation, as discussed below.

1. Cybersecurity policies need to be consistent with data governance policies

Section 500.03 of 23 NYCRR 500 specifically requires that cybersecurity policies address "data governance and classification." For example, cybersecurity policies relating to data ownership need to be consistent with any data governance roles, such as "data owner" and "data custodian."

2. Critical data elements need to consider cybersecurity requirements

Most financial services companies have spent enormous sums of money identifying critical data elements (CDEs), such as "Probability of Default" for CCAR and DFAST. The CDE program also needs to consider cybersecurity requirements. For example, Section 500.01(g)(1) includes a partial inventory of nonpublic information, such as Social Security number, driver's license number, account number, credit card number, debit card number, and biometric information.

3. The metadata hub needs to be synchronized with IT asset inventory and access control

Section 500.03 deals with cybersecurity policies for asset inventory. Section 500.07 deals with access privileges to information systems. The data governance program must ensure that the metadata hub has an inventory of applications that is consistent with the IT asset inventory tool (such as ServiceNow®).

4. Improve the quality of information within IT asset inventory

Data governance needs to work with IT to improve the quality of information within the IT asset inventory, such as ServiceNow. For example, the asset inventory should include an application's production, development, testing, and disaster recovery instances, especially if they contain sensitive information. In addition, the names of application owners must be kept updated to support periodic review of access privileges as required by Section 500.07.

5. Data retention

Section 500.13 requires covered entities to have cybersecurity programs that include policies and procedures for the secure disposal, on a periodic basis, of nonpublic information unless otherwise required by law or regulation. As a result, cybersecurity programs need to be tightly aligned with information lifecycle management.

About the Author

Sunil Soares is the founder and managing partner of Information Asset. He is a counsel to several chief data officers. Sunil is the author of several books, including The IBM Data Governance Unified Process, Selling Information Governance to the Business, Big Data Governance, IBM InfoSphere: A Platform for Big Data Governance and Process Data Governance, Data Governance Tools, The Chief Data Officer Handbook for Data Governance, Data Governance Compliance for BCBS 239 and DFAST, and Data Sovereignty and Enterprise Data Management: Extending Beyond the European Union General Data Protection Regulation. Prior to this role, Sunil was the director of information governance at IBM.

Information Asset is a services firm focused on data governance and enterprise data management. For more information, please visit www.information-asset.com.

Want to learn more? Please visit us at **www.information-asset.com**.
Contact us today at **sales@information-asset.com**.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor is it subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.