BTB SECURITY

CYBERSECURITY IN NEW YORK STATE

REMAINING COMPLIANT WITH EMERGING REGULATIONS

The financial industry is a significant cybersecurity target. With this in mind, the New York State Department of Financial Services (DFS) implemented Cybersecurity Regulation 23 NYCRR Part 500 in response to "the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations, and independent criminal actors."

KEY DATES

AUGUST 28, 2017
The 180-day transition ends. Covered Entities must comply unless otherwise specified.

SEPTEMBER 27, 2017
The 30-day period for filing Notices of Exemption ends. Covered Entities that qualify must file a Notice of Exemption.

FEBRUARY 15, 2018
Covered Entities must submit certification under 23 NYCRR 500.17(b).

MARCH 1, 2018
The 12-month transition ends. Covered Entities must comply with 500.04(b), 500.05, 500.09, 500.12, and 500.14(b).

SEPTEMBER 3, 2018
The 18-month transition ends. Covered Entities must comply with 500.06, 500.08, 500.13, 500.14(a) and 500.15.

MARCH 1, 2019
The 24-month transition ends. Covered Entities must comply with 500.11.

BACKGROUND & SCOPE

The serious nature of cybercrime—including the risk to both industry and consumers—warrants standards that are effective yet not prescriptive. The regulation indicates cybersecurity programs match risk and align to technological advances to protect Information Technology (IT) systems and sensitive customer information. Regulations require organizations assess their own risks—and design programs to address them. Each organization must implement a program to protect both the institution and customers. This includes annual filing to certify compliance and provides important protections.

THESE INCLUDE:

- Controls for a cybersecurity program including requirements for a program that is adequately funded and staffed, overseen by qualified management, and reviewed by the most senior governing body of the organization
- Risk-based minimum standards for technology systems including access controls, data protection including encryption, and penetration testing
- Required minimum standards to help address any cyber breaches including an incident response plan, preservation of data to respond to such breaches, and notice to DFS of material events
- Accountability by requiring identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance to DFS

WHO DOES 23 NYCRR EFFECT?

Cybercrime exploits vulnerabilities to access sensitive data, causing significant losses—including consumers who find private information revealed, stolen, or used improperly. According to DFS, Covered Entities are "any Person operating under or required to operate under a license, registration, charter, permit, certificate, accreditation, or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law." In practical terms, this means all businesses operating within New York State.

THAT INCLUDES:

- BANKS, TRUSTS, CREDIT UNIONS, SAVINGS AND LOANS, AND CHECK CASHERS
- INSURANCE COMPANIES—INCLUDING ACCIDENT, CASUALTY, HEALTH, LIFE, AND PROPERTY
- HOLDING OR INVESTMENT COMPANIES—INCLUDING LENDERS OR MONEY TRANSMITTERS
- MORTGAGE BANKERS, BROKERS, ORIGINATORS, AND SERVICERS
- PREMIUM AND SALES FINANCE AGENCIES OR COMPANIES
- OTHER BUDGET PLANNERS, FOUNDATIONS, CORPORATIONS, AND SAFE DEPOSIT COMPANIES

HOW IS 23 NYCRR 500 DIFFERENT?

> Very few organizations or industries do not do business with or in New York State, meaning this regulation ultimately influences the entire nation."

While either the Federal Government or industry groups have enacted other regulations, the fact that this regulation comes from the State level also sets it apart. This marks the first time a state has pushed for such regulation. Given the role New York plays in the financial sector, this is fitting. In the future, do not be surprised to see when other states enact their own cybersecurity measures. While this is a statesponsored regulation, the effects are certainly wide reaching. Very few organizations or industries do not do business with or in New York State, meaning this regulation ultimately influences the entire nation.

PUTTING REGULATIONS IN PLACE

The risk of cyberattack is severe, making regulation a priority. New York is a signatory to an agreement among state regulators addressing interstate branching. The home state of a bank with branches in New York is primarily responsible for supervision of all branches.

In cooperation, DFS provides coordination and assistance—maintaining the right to examine New York branches. They encourage all financial institutions—including out-of-state banks—to adopt 23 NYCRR 500. The full text appears here for reference.

AS IMPLEMENTED, 23 NYCRR 500 REQUIRES THAT COVERED ENTITIES:

- Adopt comprehensive cybersecurity—including documentation, procedures, and response.
- Identify a Chief Information Security Officer (CISO) to report annually on cybersecurity risk.
- Annually submit certification of compliance—keeping documentation, evidence, and records for five years.
- Encrypt or secure nonpublic information on external networks by approved means.
- Perform annual penetration testing and biannual vulnerability assessments.
- Notify the Superintendent within 72 hours of any event likely to harm operations.
- Document secure application development and review as necessary.
- Maintain five years of transaction records and three years of audit trails.
- Maintain a data retention and disposal program based on regulatory requirements.
- Perform periodic risk assessment on IT systems and non-public information.
- Evaluate third-party practices—including periodic risk assessment.
- Employ qualified, adequately trained cybersecurity personnel.
- Verify that security staff remains current on threats and countermeasures.
- Limit user access, periodically review access, and monitor unauthorized activity.

FACING THE CHALLENGE OF COMPLIANCE

The primary challenges of 23 NYCRR 5000 are the push for annual certification and the need to designate a Security Officer. While previous regulations have called for only the monitoring of critical devices or applications, 23 NYCRR 500 is far more holistic in scope.

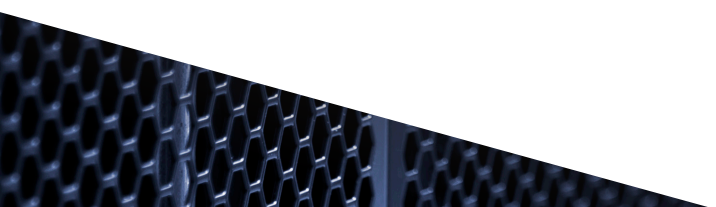
This regulation also calls for organizations to not only monitor and identify threats, but requires the capability to respond as well. Another concern is the fact that organizations may have put off assembling what they need to assess the needs of this regulation—and now find themselves scrambling to meet requirements.

THE KEY TAKEAWAY

Remember that this is a baseline set of controls. Other regulations or industry standards have tried to assemble very specific sets of rules that—while comprehensive in nature—have ultimately missed the mark in some way.

What New York State has assembled is very broad. It is more of a framework, leaving specific actions and policies up to the entities themselves. This flexibility in meeting standards should prove more beneficial to those affected in the end—enabling organizations to find the solutions that work best for their business.

> This regulation also calls for organizations to not only monitor and identify threats, but requires the capability to respond as well."



ABOUT THE AUTHOR

Ron Schlecht, Jr. is the Founder and Managing Partner of BTB Security, a specialized cyber security services firm that specializes in proactively detecting threats as well as defending against and defeating cyber security adversaries. His background in law enforcement, information security, and forensics helps organizations shield their assets, customers, and employees against security breaches.

RON SCHLECHT, JR.
(CISSP, CCE)

WHAT WE DO

BTB Security helps organizations worldwide detect, defend and defeat security breaches. From ethical hacking and vulnerability assessments to comprehensive managed security services programs, incident response and forensic analysis, BTB's solutions are designed to provide comprehensive security to organizations of all sizes.

BTB SECURITY