CYBERSECURITY SOLUTIONS FOR FINANCIAL SERVICES

23 NYCRR 500

Financial institutions are coming under increased scrutiny and regulation in response to the continuously evolving cyber-threat landscape. Meeting the challenges of requirements such as New York State's 23 NYCRR 500 can stretch already overworked IT staff to the breaking point. Fortunately, SageNet's cybersecurity practice can provide end-to-end information security solutions tailored to your organization's specific needs and capabilities.

WHAT IS NY DFS 23 NYCRR 500?

Effective March 1, 2017, the New York Department of Financial Services (DFS) regulation 23 NYCRR 500 requires organizations operating under the state's banking, insurance, or financial services laws to develop a comprehensive cybersecurity program. Among the regulation's requirements, the organization must:

- Establish and manage multiple cybersecurity programs
- Document the organization's cybersecurity capabilities
- Appoint a designated Chief Information Security Officer (CISO) (may be a third-party)
- Perform a risk and gap analysis
- Create a centralized repository of cybersecurity data
- Perform and submit annual regulatory audits
- Document cybersecurity activities and initiatives
- Quickly and effectively respond to cybersecurity events
- Notify the DFS within 72 hours of certain cybersecurity events
- Require the CISO to submit semi-annual reports to the board of directors

SageNet can help organizations meet and exceed the requirements of 23 NYCRR 500 with a comprehensive cybersecurity program based on the principles of an ISO 27001/27002 or NIST 800-53 framework.

SageNet Cybersecurity and Consulting Services provide financial organizations access to an experienced cybersecurity team. SageNet cybersecurity analysts, engineers and architects are certified, qualified and armed with a suite of specialized security tools and solutions as well as three U.S.-based 24x7x365 Network Operations and Security Operations Centers.

Features

- Security Program Assessments (ISO 27002, NIST 800-53)
- Cyber Threat Mitigation & Response Planning
- Managed SIEM
- IPS, Firewall, Web & Mail Filter, Data Loss Prevention
- Penetration Testing – Network, Web App & Mobile
- 24x7x365 Security Operations Center
- Virtual CISO Services
- Enterprise Risk Management

sageSECURE™

From information security program design, to risk management, to daily managed security operations, SageNet Cybersecurity and Consulting Services can help transform your organization from a security checkbox mentality to a culture of pursuing security best practices.

ASSESSMENTS

SageNet can provide information security program assessments that are rooted in the framework of ISO 27001/27002, or NIST 800-53. In addition, SageNet can incorporate other compliance regulations such as PCI or HIPAA into the assessment process to meet specific industry vertical requirements. SageNet security assessments include interviews of key stakeholders, an evaluation of technical security controls, toolsets, and business process of the corporate, as well as remote location environments.

Using industry best practices and our own proprietary tools and methodologies, SageNet cybersecurity assessments identify potential vulnerabilities with their associated risk, and deliver actionable recommendations to strengthen security, reduce risk, and better protect against both internal and external threats.

PLANNING & PROGRAM DESIGN

SageNet can help create a security function within an organization or assess and enhance the controls in place within an existing security program. The first step to developing or enhancing a security program is to understand its current state, the compliance requirements, and the current controls as well as business processes in place to protect sensitive information and systems. SageNet begins these engagements with a program assessment specifically tailored to your organization and then helps design and implement the security program that will advance your organization's security posture.

VIRTUAL CISO

It is critically important for any organization to implement the proper security strategy and controls. Many organizations lack the resources needed to understand the technical and business requirements of an effective security program that is appropriate for their company. Architecting the security program and making the right decisions around what investments are needed is often a challenge.

As an ongoing managed service, SageNet can provide senior-level Chief Information Security Officer (CISO) services to assist with security program leadership, strategy, execution, and oversight. All members of the CISO team at SageNet are certified CISSP's and have held senior security leadership roles within large companies. Virtual CISO services include:

- Security Planning & Program Design
- Information Risk Management
- Audit Planning & Management
- Preparation & Communication with Senior Leadership & Board of Directors
- Security Program Metrics

YOUR CYBERSECURITY TEAM

SageNet works to transform your cybersecurity posture beyond fulfilling regulatory requirements to create a culture of best-practices security. We provide end-to-end information security solutions tailored to your organizations specific needs and capabilities.

To learn more about SageNet Cybersecurity Services, visit www.sagenet.com/cyber or call 866.480.2263.

Financial_DS083118