Cybersecurity for Financial Services Companies

ADDRESSING NEW YORK'S FIRST-IN-THE NATION REGULATION

New York State has implemented cybersecurity requirements for banks, insurance companies, and other financial services institutions regulated by the New York State Department of Financial Services that are designed to protect consumers' private data and ensure the safety and soundness of New York's financial services industry. If you are a financial services company operating in New York State, this document is designed to help you understand available services and technologies to support your compliance with the regulation by February 15, 2018 as required.

This document is also intended to provide guidance to proactive financial services companies outside of New York State, as this "first-in-the-nation" regulation is expected to have a domino effect in the U.S. as well as internationally.

Implementing Cybersecurity Best Practices

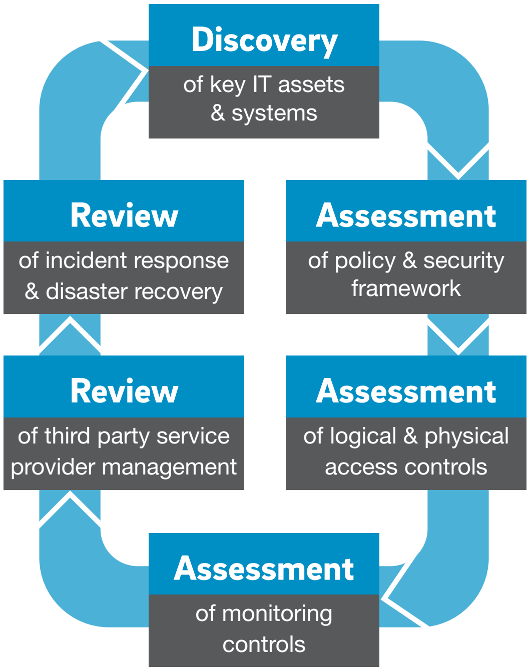
The regulation requires financial services companies to establish a cybersecurity program that is consistent with cybersecurity best practices, including:

- The identification and assessment of internal and external cybersecurity risks to the organization's non-public information
- Policies and procedures to prevent unauthorized access to the information
- Detection of cybersecurity events
- Response to any cybersecurity breaches to mitigate harm
- Recovery and business continuity
- Regulatory reporting in the event of a breach

Getting Started

As with any compliance regime, the biggest challenge for organizations is often figuring out where to begin. The regulation requires a risk assessment "sufficient to inform the design of the cybersecurity program." Trustwave can help financial organizations fulfill their risk assessment requirements and strategically implement the resulting cybersecurity roadmap with our expert consultants who help take an organization of any size through each phase of the process with the proven Trustwave methodology. The resulting assessment findings provide the basis to build or refine the most appropriate information security program for your organization. Trustwave consultants will work with you to determine the best methodology assessment framework for your business, customized to your specific business goals. A Trustwave risk assessment is right for any organization looking to assess their security risk posture and develop a risk management framework for tailored objectives.

Trustwave's risk assessment approach examines both the maturity and ongoing effectiveness of your cybersecurity program and security infrastructure through an iterative process of information gathering and vulnerability identification. It also includes assessment of third-party risk as required by the cybersecurity regulation.


Discovery
of key IT assets & systems
Assessment
of policy & security framework
Assessment
of logical & physical access controls
Assessment
of monitoring controls
Review
of third party service provider management
Review
of incident response & disaster recovery

Key Solutions for Addressing the Requirements

The risk assessment helps you build your roadmap to fulfillment of the full scope of the cybersecurity regulation, including:

- a cybersecurity policy
- penetration testing and vulnerability assessments
- system audits
- review of access privileges
- application security
- training and monitoring of personnel
- encryption of non-public information

As your risk assessor, Trustwave will provide guidance about available solutions to help you fulfill your specific requirements, including best-of-class offerings from the Trustwave security portfolio. See the next page for a summary of relevant products and services.

Trustwave offers the following products and services that can help you address the cybersecurity requirement:

Cybersecurity Program Development

Trustwave offers professional consulting services that can guide you through the development of your Cybersecurity Program as detailed by the regulation. Trustwave has the experience and methodology to guide you through the risk assessment which is an integral part of the program, help you identify gaps that need to be addressed, and to build out your full program as specified.

Cybersecurity Risk Assessment

A Trustwave Information Security Risk Assessment can help you meet your cybersecurity compliance obligations and gain an understanding of your exposure to threats and vulnerabilities through risk identification and risk mitigation prioritization for your key assets and systems, policies, procedures and controls across business units. As defined by the regulation, the results of the risk assessment will inform the development of the Cybersecurity Program.

Cybersecurity Policy Development Consulting

Trustwave offers Policies and Procedures services that can assist in the development of a Cybersecurity Policy to address the requirement. This policy development will encompass each specified element, such as data governance and classification, physical security and environmental controls, and vendor and third-party service provider management as detailed in the regulation.

Security Awareness Education

Our cloud-based Security Awareness Education gives your organization the tools they need to help protect your data from cybersecurity threats. The courses can be tailored to your organization and key roles within the organization. It includes lessons specific to Banking Security.

Secure Development Training

Trustwave offers two different training formats to help you address the application security requirement for developing secure in-house applications:

- comprehensive online Secure Development Training (SDT) for your developers, engineers and IT personnel
- onsite secure development training delivered by the SpiderLabs team at Trustwave

Risk-based Authentication/Access Privileges

Trustwave consulting services can help you ensure that your risk-based authentication and access privileges adhere to the specifications of the requirement. Trustwave also offers a number of solutions that can help you determine that information access is limited to the necessary personnel.

Incidence Response & Readiness

The Trustwave Incident Readiness (IR) Program helps you prepare for, recognize, train and act based on procedural methods when an incident takes place to reduce its impact. Experts from the Trustwave SpiderLabs Global Incident Response Team will deploy to a compromise to assist you. The Trustwave IR Program's structure is based on our investigations of thousands of data breaches and responses to hundreds more each year.

Managed Security Testing

Trustwave Managed Security Testing (MST) reveals your vulnerabilities across scanned assets and provides remediation guidance so you can make good risk management decisions and technology investments. Businesses use Trustwave Managed Security Testing as a single platform for their managed vulnerability assessment, database security testing, network penetration testing and application penetration testing needs.

Audit Trails

Trustwave consulting services can help you ensure that you are maintaining and retaining audit trails as required. Trustwave also offers a number of solutions that offer auditing capabilities for transactions. These include Managed Endpoint Detection and Response (EDR), AppDetectivePRO, DbProtect Activity Monitoring, SIEM Enterprise, SIEM Log Management Enterprise, Managed SIEM services, Web Application Firewall and Windows Log Collection.

Managed Security Services

Trustwave offers a wide range of Managed Security Services which includes prevention and defensive services such as managed firewalls, managed intrusion prevention systems and managed gateways for web, email and other sensitive services.

Additionally, Trustwave offers a robust suite of services for security monitoring, detection and response that combines a number of solutions to provide a comprehensive approach to advanced threat detection.

Third-Party CISO Services

The Trustwave Virtual CISO service gives you a customizable solution to get the level of Chief Information Security Officer (CISO) services you need. Working with your senior management team, Trustwave can manage a program that protects your organization in accordance with the requirements.

Database Security Solutions

AppDetectivePRO and DbProtect comprise the industry's most comprehensive database security solution and empower you to assess, monitor and protect your most critical database assets while simplifying audits, monitoring risk, and automating your compliance requirements. AppDetectivePRO is designed for point-in-time scans while DbProtect is a highly scalable solution for the enterprise.

Web Application Firewall (WAF)

Trustwave Web Application Firewall (WAF) provides real-time event monitoring and protection against web application attacks, virtual patching and data masking to help meet compliance for industry regulations. Continuous monitoring will assist in identifying security events and application vulnerabilities that can be added to security processes. Virtual patching and data masking allow an organization to reduce the need for ad-hoc patches and allows vulnerabilities to go through the normal development cycle. Detail reports can provide management with view to application security posture and auditing for compliance.

For more information, see Financial Services.

Trustwave®

For more information: www.trustwave.com