23 NYCRR 500 AND TRIPWIRE SOLUTIONS

"FIRST IN NATION" CYBERSECURITY LEGISLATION FOR FINANCIAL INSTITUTIONS

◆ ... designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. ◆

The financial services market is a key target for cyber criminals given potential financial rewards. Their motives can also be political since financial systems are critical infrastructure for society. The New York State Department of Financial Services (DFS), the regulatory body that oversees financial services companies licensed by or operating in the state, has been closely observing the ever- growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors.

DFS has mandated new rules, Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, or 23 NYCRR 500 for short, that require the financial services organizations covered and licensed by them to establish and maintain a cybersecurity program. The regulation was developed based on a survey of regulated banking

institutions and insurance companies, and consultations with cybersecurity experts. While 47 states in the US have adopted different breach notification statutes, individual states have not yet adopted broad cybersecurity mandates; New York is the first. "… designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion." (www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf)

The effective date for the new regulation is March 1, 2017, and covered entities have 180 days from that date to comply with the rules. A further requirement to provide a Certification of Compliance to the DFS will commence January 2018. The regulation language does not include fines if entities are not in compliance, but DFS has a reputation for levying steep fines.

"Although still much more prescriptive than what we've seen out of other regulators, the revised regulations are now more flexible and tied more closely to each organization's particular risk assessment," said Edward McAndrew, a partner at Ballard Spahr, who serves as co-leader of his firm's Privacy and Data Security Group. "That said, they have teeth and will require substantial investment of time and resources to ensure initial and ongoing compliance. … I fully expect other states to follow suit with similar regulations both in the financial services and other industries." (www.scmagazine.com December 29, 2016)

ACHIEVE 23 NYCRR 500 COMPLIANCE WITH TRIPWIRE

Tripwire has a proven track record with many cybersecurity regulations (e.g. PCI, NERC CIP, SOX, HIPAA) and frameworks (e.g. NIST, CSC 20). Tripwire automates cybersecurity regulatory compliance, allowing organizations to not only achieve compliance but also reduce time spent preparing for and maintaining compliance through continuous monitoring and audit-ready evidence. In addition, Tripwire offers an open architecture with integrations to many other tools to enhance security and operations.

The new DFS regulations require that organizations take a programmatic, risk-assessment based approach to secure non-pubic information and the organization's information systems. Tripwire's suite of products can provide specific required controls, validate that organizations are in compliance with the standard, and support compliance by providing relevant data and reports. Tripwire's core capabilities for integrity monitoring, policy compliance, vulnerability management and centralized log collection are vital to achieving and maintaining compliance with 23 NYCRR 500.

> ***That said, (the regulations) have teeth and will require substantial investment of time and resources to ensure initial and ongoing compliance. … I fully expect other states to follow suit with similar regulations both in the financial services and other industries.***
>
> **EDWARD MCANDREW, PARTNER, BALLARD SPAHR**

Mapping of 23 NYCRR 500 to Tripwire Products

Requirement /Description	How Tripwire can help[1]	Tripwire Enterprise	Tripwire IP360	Tripwire Log Center	Tripwire Overall
500.02 - Cybersecurity Program					
(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts; stored on those Information Systems, from unauthorized access, use or other malicious acts; (3) detect Cybersecurity Events; (4) respond to identified or detected Cybersecurity Events to mitigate any negative effects; (5) recover from Cybersecurity Events and restore normal operations and services; and (6) fulfill applicable regulatory reporting obligations.	The Tripwire suite of products provides detailed information about the environment, including changes, configuration, inventory, vulnerability risk and log data. This information can be used by customers to create more accurate risk assessments and identify cybersecurity incidents.	**Supports**	**Supports**	**Supports**	**Supports**
Section 500.03 Cybersecurity Policy.					
(a) Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: (1) information security; (2) data governance and classification; (3) asset inventory and device management; (4) access controls and identity management; (5) business continuity and disaster recovery planning and resources; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data privacy;(12) vendor and Third Party Service Provider management; (13) risk assessment; and (14) incident response.	Tripwire's suite of products provides the ability to measure and manage risk, ensuring confidentiality, integrity and availability. When applied to processing systems, Tripwire can monitor systems against security policies, identify and track vulnerabilities, and provide the ability to investigate activity through log data.	**Provides**	**Provides**	**Provides**	

Mapping of 23 NYCRR 500 to Tripwire Products

Requirement /Description	How Tripwire can help[1]	Tripwire Enterprise	Tripwire IP360	Tripwire Log Center	Tripwire Overall
500.05 - Penetration Testing and Vulnerability Assessments					
(a) The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments, and shall be done periodically. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:(1) annual penetration testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and (2) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.	Tripwire IP360 can provide continuous and periodic vulnerability assessment to comply with this requirement. Tripwire Enterprise can provide continuous, even real-time, monitoring of changes on systems in the environment. Tripwire Log Center can provide continuous monitoring of logs and log events across the environment.	**Provides**	**Provides**	**Provides**	**Provides**
500.06 - Audit Trail					
(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. (b) Each Covered Entity shall maintain records required by this section for not fewer than five years.	Tripwire Enterprise and Tripwire Log Center can collect change and log data to support the investigation of incidents and the reconstruction of transactions.	**Supports**		**Supports**	**Supports**
500.07 - Access Privileges					
As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	Tripwire Enterprise can validate that systems are configured to limit user access privileges. Tripwire Log Center and Tripwire Enterprise can be used to alert based on user activity that violates this policy.	**Validates**		**Validates**	**Validates**

Mapping of 23 NYCRR 500 to Tripwire Products

Requirement /Description	How Tripwire can help[1]	Tripwire Enterprise	Tripwire IP360	Tripwire Log Center	Tripwire Overall
500.09 - Risk Assessment					
(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.	The Tripwire suite of products provides detailed information about the environment, including changes, configuration, inventory, vulnerability risk and log data. This information can be used by customers to create more accurate risk assessments and identify cybersecurity incidents.	**Supports**	**Supports**	**Supports**	**Supports**
(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;	Tripwire Enterprise can provide a mechanism for categorizing assets through asset tags. Tripwire IP360 can feed additional data into that categorization system through integration with Tripwire Enterprise.	**Provides**	**Supports**		**Provides**
500.12 Multi-Factor Authentication.					
(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.	Tripwire Enterprise can validate that multi-factor authentication is configured on systems. Tripwire Log Center can identify a number of authentication events in log data to alert on misuse.	**Validates**		**Supports**	**Validates**
(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.	Tripwire Enterprise can validate that multi-factor authentication is configured on systems. Tripwire Log Center can identify a number of authentication events in log data to alert on misuse.	**Validates**		**Supports**	**Validates**
500.14 - Training and Monitoring					
(1) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and	Tripwire Log Center can identify and alert on user activity from logs, providing the ability to identify abuse, misuse and miconfigured authentiction. Tripwire Enterptise has the ability to detect unauthorized users tampering with Nonpublic information	**Provides**		**Provides**	**Provides**

Mapping of 23 NYCRR 500 to Tripwire Products

Requirement /Description	How Tripwire can help[1]	Tripwire Enterprise	Tripwire IP360	Tripwire Log Center	Tripwire Overall
500.15 Encryption of Nonpublic Information.					
(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	Tripwire Enterprise can be used to validate that encryption is in place.	Validates			Validates
(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.	Tripwire Enterprise can be used to validate that the alternative controls are in place, and provide evidence to auditors. To the extent that an alternative control includes monitoring systems for changes or collecting logs, Tripwire Enterprise and Tripwire Log Center can provide those controls.	Validates		Supports	Validates
(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.	Tripwire Enterprise can be used to validate that the alternative controls are in place, and provide evidence to auditors. To the extent that an alternative control includes monitoring systems for changes or collecting logs, Tripwire Enterprise and Tripwire Log Center can provide those controls.	Validates		Supports	Validates
500.17 - Notices to Superintendent					
(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event as follows has occurred:	Tripwire's suite of products provide detailed data that can help determine whether a cybersecurity event has occurred and whether that event is likely to cause material harm.	Supports	Supports	Supports	Supports

◆ Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

SBNYCRR1a 201704