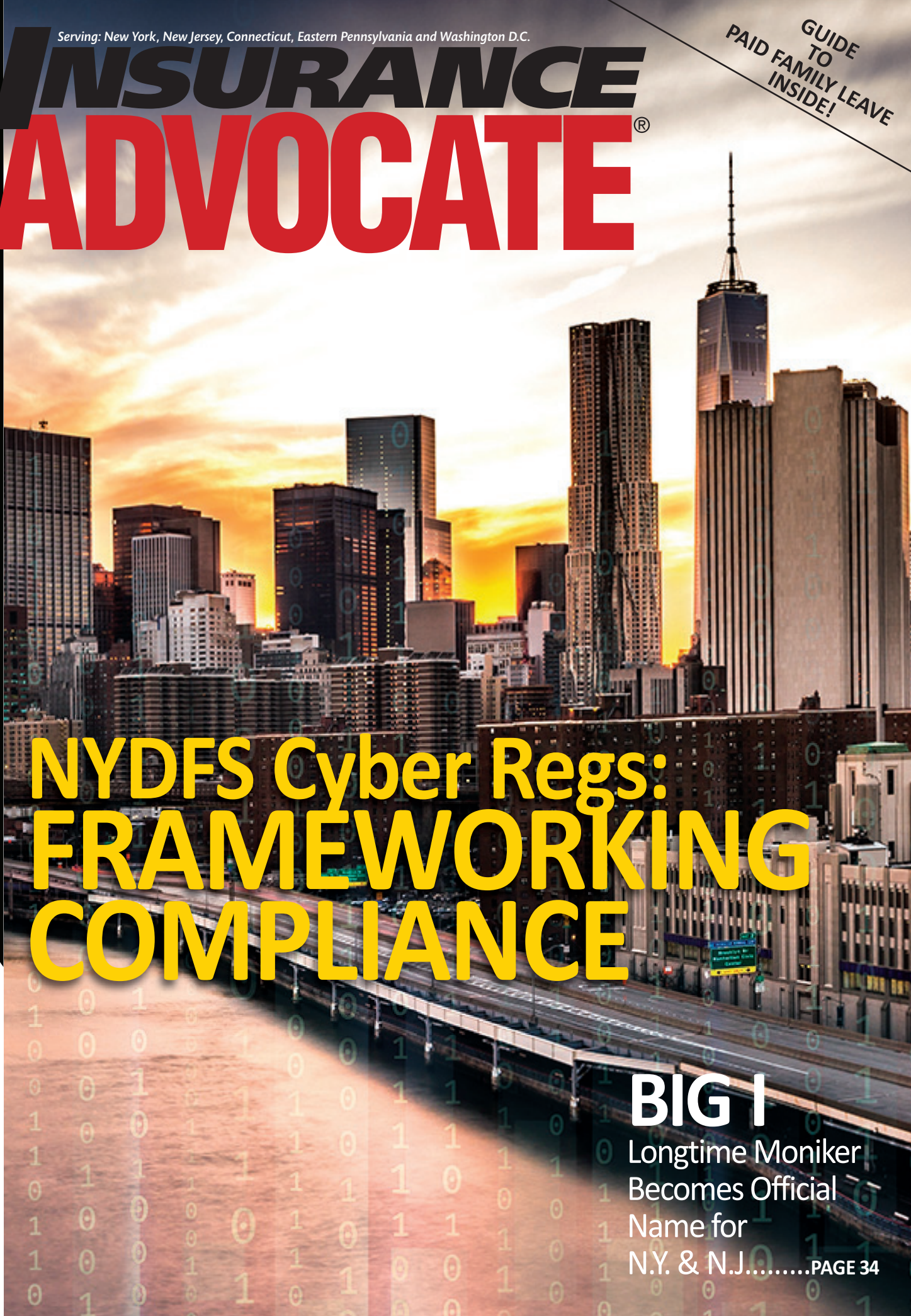
Serving: New York, New Jersey, Connecticut, Eastern Pennsylvania and Washington D.C.

INSURANCE ADVOCATE®

GUIDE TO PAID FAMILY LEAVE INSIDE!



NYDFS Cyber Regs: FRAMEWORKING COMPLIANCE

BIG I

Longtime Moniker Becomes Official Name for N.Y. & N.J......PAGE 34

Vol. 128 No. 15 | September 25, 2017

Book your cyber health checkup now to find out where you stand.

What you don't know could hurt you.

NYS DFS CHECKUP™

SPECIAL OFFER

SIGN UP BEFORE NOV 30 2017
35% DISCOUNT*
PROMO CODE: **NYSDFS-OFFER17**

SIGN UP BEFORE JAN 31 2018
20% DISCOUNT*
PROMO CODE: **NYSDFS-OFFER18A**

SIGN UP BEFORE JUNE 30 2018
10% DISCOUNT*
PROMO CODE: **NYSDFS-OFFER18B**

*Discount is off list price and cannot be used with any other discount or offer.

- ✓ How will you satisfy the new requirements without breaking your budget?
- ✓ Do you know which items need attention to become compliant?
- ✓ How do you prioritize requirements?
- ✓ Do you have a trustworthy cybersecurity partner who understands the insurance industry and works well with your legal advisors?

The NYS DFS Checkup™ is quick, easy, affordable and available online.

Take Your First Step to Compliance Today:

www.assured.enterprises/NYSDFS-OFFER17

ASSURED ENTERPRISES INC

www.assured.enterprises

Assured Enterprises, Inc. is a cyber risk assessment, measurement and mitigation company with innovative proprietary tools and cost efficient solutions. **AssuredScanDKV®** is the only tool capable of detecting known vulnerabilities in the software on your network. It's the best solution to satisfy vulnerability scanning (23 NYCRR Section 500.05).

NYDFS Cyber Regs: Frameworking Compliance

BY STEPHEN M. SOBLE

security compliance

By now, we should all be aware of the sweeping cybersecurity compliance regulations passed by the NYS Department of Financial Services, which is "designed to assess the effectiveness" of a wide array of Covered Entities. Broadly speaking, these entities include banking, insurance, financial advisory and financial management companies operating in NYS, satisfying some minimal footprint definitions (10 or more employees or $5 Million in NYS based revenue or $10 Million or more in global turnover). The risks of non-compliance are stern—fines, potential criminal penalties, injury to reputation, loss of reputation and clients, not to mention public ridicule. DFS and the NYS Attorney General will strive to set a few examples to stimulate voluntary compliance—classic new regulatory adoption planning.

It is interesting to note that insurance policies which cover certain types of negligence, errors and omissions, may find that the documentation and compliance requirements actually serve to mitigate the scope of coverage in the event of a data breach. However, it will take a few real-world cases and some deeper legal analysis to see precisely how this plays out.

Stephen M. Soble is Chairman and CEO of Assured Enterprises, Inc. He is a graduate of Harvard Law School, is a member of the NYS bar. Nothing stated herein is intended to be and should not be construed to serve as legal advice. Please consult your legal counsel. Assured Enterprises is a premier Cyber Risk Assessment, Measurement and Mitigation company, inventor of innovative products and solutions for the US Government and private sector.

Recognize What is Minimally Required, When it is Required and What Might be Practically Recommended

We have prepared a chart in the two-page tear out addressing the timing of each requirement and some other details of various critical points noted below. However, as we see it, the regulatory compliance essentials are:

- A NYS DFS cyber compliance checkup to define your company's compliance status today.
- An annual cybersecurity risk assessment—the more comprehensive the more prepared you will be to handle the other requirements (Sec. 500.01 (k) and (l); Sec. 500.09)
- Threat assessment, especially addressing hacking from "nation-states, terrorist organizations and independent criminal actors" (Sec. 500.00)
- Written compliance and response Programs, Policies and Procedures (Sec. 500.02/03/16)
- Report to the Superintendent of DFS "cybersecurity events" (breaches, attempted breaches, successful or not, originating from any source including but not limited to insider actions, accidents and more) entailing access, disruption or misuse of information or an Information System (sec. 500.17) ***now in effect***
- Continuous monitoring or periodic Penetration Testing and vulnerability assessments (Sec. 500.05/08; see Sec. 500.01 (h)), augmented by annual testing and reviews to determine improvements (remediation) based on the prior assessments (Sec. 500.05 (a))
- Bi-annual vulnerability assessments, including scans "reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems, based on Risk Assessment." (Sec. 500.05(b))
- "Written procedures, guidelines and standards designed to ensure the use of secure development practices", especially for any proprietary applications (software) and "procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity, within the context of the Covered Entity's technology environment." (Sec. 500.08)
- Appointment of a responsible senior member of the company, such as a CISO to monitor all matters and to report to the Board of Directors or equivalent. May substitute a Third Party Virtual CISO to fulfill this requirement. The CISO (virtual or

It is interesting to note that insurance policies which cover certain types of negligence, errors and omissions, may find that the documentation and compliance requirements actually serve to mitigate the scope of coverage in the event of a data breach.

CONTINUED ON PAGE 16

CONTINUED FROM PAGE 15

FTE) of the Covered Entity, must monitor and maintain documentation. (Sec. 500.04)
- Develop a training and monitoring program for employees (Sec. 500.10; Sec. 500.14)
- Develop a Security Policy and system for your supply chain (third party service providers)
- Implement Multi-Factor Authentication (Sec. 500.12)
- Devise and implement a Data Retention Policy, consistent with other legal requirements (Sec. 500.13)
- Adopt encryption of Nonpublic Information (Sec. 500.15)
- Establish a written incident response plan (Sec. 500.16)
- ***If you qualify for a limited exemption, the filing due date for the form is September 27, 2017***

Practical Tips for Managing Compliance and Improving Your Security

- Get started now, recognizing that some requirements phase in over time. See our chart in the tear out supplement.
- **Determine whether you can handle all requirements** in-house or if you need help.
- If you need help, **Identify the Team** to cost efficiently address the requirements. *See our section in the tear out supplement addressing issues in deciding which outside team is right for you.*
- **Recognize that it takes a village.** If you need outside cybersecurity compliance help you will need at a minimum a qualified cybersecurity engineering firm and competent outside legal counsel going forward. The cybersecurity engineering firm should be able to provide most of the compliance and advice, but it is always good to consult with outside counsel on strategies, defensive postures, plans, policies and procedures. One good way to save money is to instruct outside counsel to review rather than draft policies, procedures, training programs and response protocols and plans.
- **Stop and Smell the Roses**. After completion of each phase of your compliance with the new regulations, re-evaluate where you are, where you are going and whether your plans are seamlessly integrated into your operational efficiency. A bit of forethought will go a long way to reducing the stress associated with managing a breach should one occur.
- **Recognize that Compliance does NOT Equal Security.** Devise the steps to improve your company's cyber health while conducting compliance requirements.
- **Consider the comparable cost of off-the-shelf, one size fits all solutions** compared with a more tailored, customized approach which focuses on operational efficiency and cost mitigation over the reasonable medium term.
- **Understand that Risk Assessment, Measurement and Mitigation is the real goal** of the new regulations and that, subject to advice of counsel, steps which you take to address the spirit of the law may improve the flexibility in addressing a technical deficiency in documentation or ministerial compliance requirements.

Welcome to the new norm defining one of the costs of doing business in The Digital Age. The regulations are a part of the landscape and when compared to other regimes, such as the European Union's General Data Protection Regulation (which we will address in a future column), the NYS DFS Cybersecurity requirements are straightforward and less Draconian.[IA]

Make Secure Operations and Compliance Routine, Going Forward

Learn More About Assured Solutions:
www.assured.enterprises

...the NYS DFS Cybersecurity requirements are straightforward and less Draconian.

A Practical Guide to Compliance with Key Elements of the NYS DFS Cybersecurity Regulations 23 NYCRR Part 500

DEADLINE	REQUIREMENT	23 NYCRR REFERENCE	HOW ASSURED CAN HELP
Mar 1 2017	Law becomes effective, with transition period.	Section 500.21 and 500.22	Fully prepared **NYS DFS Checkup™**, **Cyber Health Essentials Checkup™** or **TripleHelix™** and much more.
Aug 28 2017	180-day transition ends. Law in full effect except as provided below. NOTE: Notices of a breach to Superintendent within 72 hrs of discovery and defined third-party notice enforced.	Section 500.22	Data breach notification provisions apply. Prepared to assist with Breach Response Team. How can you find a breach today? **AssuredScoutRWT™** and **AssuredHawkDCM™** available for sophisticated networks.
Sep 27 2017	Last day to file Notice of Exemption.	Section 500.19(e) and Section 500.01(c) Form in Appendix B, page 14	Applies to micro-sized companies only. See definition of "Covered Entities." No cybersecurity engineering requirement.
Feb 15 2018	First annual filing: written statement of CISO or Virtual CISO regarding compliance submitted to Superintendent signed by Board Chair or Senior Officer.	Section 500.17(b) Appendix A, page 13	Assured's **NYS DFS Checkup™** online offering tells you where you stand. Assured can provide Virtual CISO, services and guidance on how best to cost efficiently comply.
Mar 1 2018	CISO reports to board of directors on the Covered Entity's cybersecurity program and risks; policies and procedures in place.	Section 500.04(b)	Assured supports all reports and provides virtual CISO services.
	Penetration testing and vulnerability assessments.	Section 500.05	Pen testing and **AssuredScanDKV®** provide full compliance. DKV is the only deep software scanner on the market. It helps you eliminate some 80% of the known software vulnerabilities on your network; makes bi-annual vulnerability assessments easy and effective.
	Risk assessment.	Section 500.09	**NYS DFS Checkup™** to see where you stand. **Cyber Health Essentials Checkup™**—a complete assessment online for mid-sized clients. **TripleHelix™** is the most comprehensive cyber risk assessment on the market. It allows add-on of other required regulatory/compliance reports. Includes a **CyberScore®**—the most refined benchmarking/measurement tool for cyber risk insurance currently available. Reports, roadmaps and **Regulatory Compliance Dossier** included. Most comprehensive compliance with NYS DFS available in the Dossier.
	Multi-factor authentication.	Section 500.12	Assured provides both off-the-shelf third party solutions or Assured's own solutions. You decide what works for you.
	Cybersecurity awareness training.	Section 500.14(b)	Assured provides compliant training program.
Sep 3 2018	Audit trail compliance.	Section 500.06	Part of optional program offering included in Virtual CISO services.
	Application security.	Section 500.08	**AssuredScanDKV®** may be used in combination with other products. With Virtual CISO services, Assured provides a complete managed solution.
	Data retention-limitation/policies and procedures.	Section 500.13	Part of optional program offering included in Virtual CISO services.
	Risk-based policies, procedures and controls.	Section 500.14(a)	Provided by **TripleHelix™**. Available as an option for all clients.
	Encryption of non-public information.	Section 500.15	Assured has state-of-the-art encryption, if needed. Encryption without key management creates its own problems. Assured's **DECENT™** encryption key management system solves any key management issues.
Feb 15 2019	Second annual filing of written statement. RE: Compliance submitted to Superintendent, signed by Board Chair or Senior Officer.	Section 500.17(b)	Included in Virtual CISO Package. Assisted by **NYS DFS Checkup™ 2019 Edition.**
Mar 1 2019	CISO reports due. Transition period ends.	Section 500.04(b)	With a sound compliance regimen firmly in place, it is time to reduce risk and begin to sleep at night.

ASSURED
ENTERPRISES INC

Copyright © 2017 Assured Enterprises, Inc. All Rights Reserved.

Assured Enterprises' Solutions

CYBERSECURITY SOLUTIONS

TripleHelix™ Framework
TripleHelix™ is the most comprehensive risk assessment system available. It gives organizations the capability to quantify, measure and benchmark their cybersecurity programs' progress.

Deliverables of a TripleHelix™ assessment:

- **Roadmap** recognizing the attributes of a sound cybersecurity system in place and recommendations for improvement;
- **CyberScore®** distills Assured's comprehensive analysis into one easy to understand number akin to a credit score; and
- **Regulatory Compliance Dossier** populated with virtually any regulatory compliance cyber report required—from NYS DFS, HIPAA to PCI to FFIEC, FISMA, GDPR and more. The Dossier eliminates the need to conduct multiple assessments to address multiple compliance requirements.

NYS DFS Checkup™
Whereas the full TripleHelix™ Framework is the solution for complex networks and large-scale companies, NYS DFS Checkup™ is a version of TripleHelix™ specifically designed for small or medium-sized companies. Through an online portal, NYS DFS Checkup™ tells you where you stand in your compliance quickly and efficiently and at an affordable cost.

AssuredScanDKV® Deep Software Scanner
As part of a TripleHelix™ assessment, we employ AssuredScanDKV® to **Detect Known Vulnerabilities** in software and to provide remediation information. AssuredScanDKV® automatically scans libraries, DLLs and executables for known vulnerabilities. It also unpacks these software elements to review the binaries. AssuredScanDKV® is a critical tool for satisfying NYS DFS biennal assessments.

DECENT™
Using blockchain technology and a patent pending invention, Assured has built a **lightweight, highly effective key management system** that allows for higher levels of encryption, yet legally warranted access to ONLY the device in question to support law enforcement activities.

The problem encountered by the FBI and Apple in 2016 has been resolved—and both privacy rights and law enforcement needs win.

Data Breach Detection, System Management Tools & Vulnerability System Management Tools
AssuredScoutRWT™, AssuredHawkDCM™ and AssuredMaestroCIS™

BIOMETRIC SOLUTIONS

Through a strategic partnership with Qafis Biometrics Technology, Assured now offers **digital identity authentication** and a comprehensive suite of biometric products (physical and behavioral) along with our state-of-the-art cybersecurity solutions.