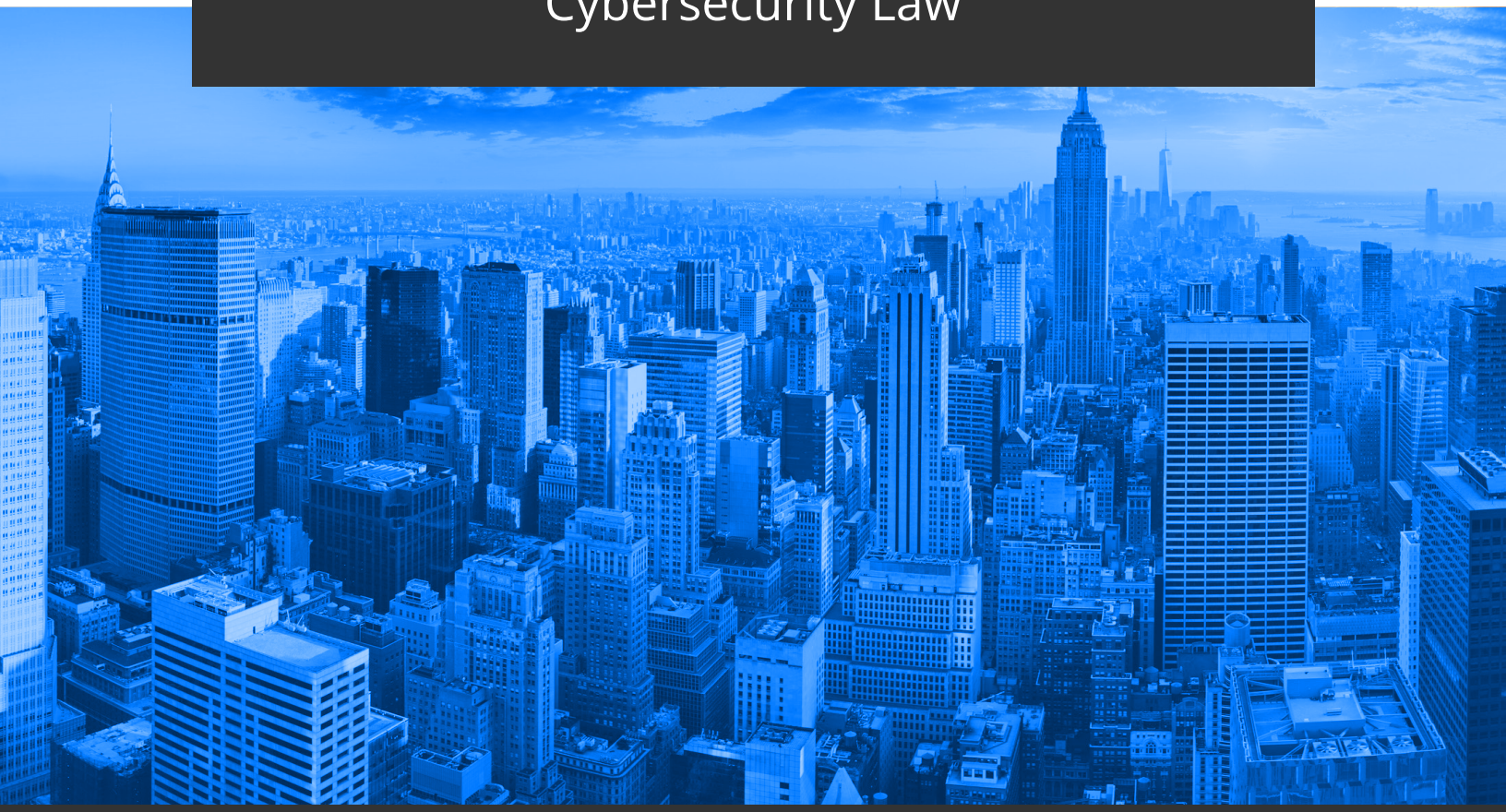
motiva

Everything You Need To Know About 23 NYCRR 500:

New York's First-In-The-Nation Cybersecurity Law



A guide for the financial sector on getting compliant – and fighting back against cybercrime

Everything You Need To Know About 23 NYCRR 500:

New York's First-In-The-Nation Cybersecurity Law

www.dfscompliance.com

(646) 374-1820

A guide for the financial sector on getting compliant – and fighting back against cybercrime

The Financial Sector Is Under Cyber Siege

Hackers are waging a war against the financial sector. And in an industry where reputation is everything – and people's most sensitive information is on the line – losing a battle carries a substantial price.

Four thousand cyber-attacks a day are threatening global financial stability. Finance is attacked 65 percent more often than any other sector – with a whopping 937 percent increase in attacks in 2016.

It only takes one data breach to ruin a financial firm's reputation as people lose trust in its ability to protect their money and most sensitive information. Sixty percent of consumers say they would stop using a bank after an online breach.

Ninety percent said they would consider legal action.

Federal regulators increasingly treat hacked companies like wrongdoers instead of victims, slapping steep fines upon businesses they believe ignored red flags or failed to take proper precautions against cybercrime.

In 2017, the first state took strong action to protect consumers from attacks with a law that is expected to serve as a model for national regulations.

New York's groundbreaking mandate – 23 NYCRR 500 – imposes stringent cybersecurity standards upon the state's financial services sector and promises hefty fines for any company who falls short.

23 NYCRR 500: It's Not As Scary As It Seems

Although some limited exemptions apply, let's be clear: Any entity regulated by New York's Department of Financial Services (DFS) must comply with at least parts of **23 NYCRR 500**.

Small business? You still need to follow many sections of the law. Headquartered elsewhere? If you do business in New York, the law applies to your company. State-chartered banks, licensed lenders, private bankers, mortgage companies and insurance companies, as well as their third-party service providers? Yes, this means you.

Here's our breakdown of how the law has New York's financial sector poised to play its part in a safer future:

- Covered entities must provide evidence that they have taken steps to safeguard the confidentiality and integrity of sensitive client data. Areas such as information security, data governance/classification, asset inventory and device management, and access controls and identity management are of the utmost importance.

- Companies must assess external and internal cyber risks, and most must create an incident response plan that details how they will respond in the event of a breach. A critical factor is how quickly the hacked business can inform DFS and consumers about the nature and scale of the attack.

- The appointment of a Chief Information Security Officer (CISO) and cybersecurity personnel is critical for most companies. The CISO can be in-house or provided by a third party. It's the CISO's duty to provide qualified expertise as the cybersecurity program is implemented, and to continually oversee its operation.

If your business hasn't begun to take action to meet these new standards, we recommend an immediate risk assessment to highlight any dangers. You should also know these deadlines (including those in the past) to avoid penalties as your company moves toward best cybersecurity practices:

March 1, 2017
23 NYCRR 500 becomes effective.

August 28, 2017
180-day transitional period ends. Covered entities must comply with the law's requirements unless otherwise specified.

October 31, 2017
Deadline for Limited Exemption filings.

February 15, 2018
Covered entities were required to submit the first certification under 23 NYCRR 500.17(b) on or prior to this date.

March 1, 2018
One-year transitional period ends. Covered entities must comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b) of 23 NYCRR Part 500.

September 3, 2018
Eighteen-month transitional period ends. Covered entities must comply with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15.

March 1, 2019
Two-year transitional period ends. Covered entities must comply with the requirements of 23 NYCRR 500.11.

A Limited Exemption Does Not Equal Limited Responsibility

The biggest myth out there is that some companies are exempt from complying with NYCRR 500. While some may be deemed small enough to escape some of the more onerous and costly parts, they must still meet many of the law's requirements.

To qualify for a limited exemption, companies must meet one or more of the following criteria:

less than 10 employees located in New York, including independent contractors

less than $5 million in gross annual revenue from business operations in New York for each of the last three fiscal years

less than $10 million in year-end total assets

Businesses who receive limited exemptions are not obligated to follow certain parts of the regulation. These include designating a CISO, encrypting or developing equivalent controls for non-public information, creating requirements for training and monitoring, using multi-factor authentication, maintaining audit trails, and writing an incident response plan.

But they are still subject to robust requirements:

- Establishing a security program and implementing cybersecurity policies
- Providing notice to DFS of cybersecurity events
- Establishing policies for the disposal of non-public information
- Limiting and periodically reviewing access privileges
- Conducting periodic risk assessments
- Implementing policies and procedures to secure information accessible to third-party service providers

Companies can lose their limited exemption if their business grows too big. All other companies are already considered non-exempt and must comply with all aspects of the law.

Why Third-Party Vendors Must Pay Attention

Companies that aren't in the financial sector can't ignore NYCRR 500. The law doesn't directly govern third-party vendors, but it demands that financial service companies insist upon robust cybersecurity measures at entities they do business with – especially those with access to critical data.

Vendors who don't comply don't face fines from DFS. But they stand to potentially lose profitable relationships with financial service customers who can't risk being held responsible for lax security measures. To comply with the law, financial firms are having to negotiate new contracts, revise old contracts, and continually monitor third-party relationships to ensure that their vendors meet best cybersecurity practices.

As part of their annual certification of compliance, covered companies must prove they are taking the right steps. Submitting a false or inaccurate certification is a serious violation and subjects the company – and possibly the person who signed or approved it – to regulatory measures and enforcement action.

For third parties who want to do business with New York's financial sector, it's time to implement best cybersecurity measures that mirror the mandates of the law. That means strong passwords, data encryption, multi-factor authentication to prevent logins from new systems and unidentified devices, and an audit trail that identifies who can see which types of data and any changes that are made.

Documented plans for detecting and promptly responding to an attack should be in place, as well as plans to ensure business continuity in the wake of an attack.

Third parties also should be willing to undergo regular cybersecurity assessments from their customers, and agree to promptly notify them after incidents occur.

Finally, vendors should take the extra step of listing and obtaining security assurances from their relevant vendors, like data center providers that provide hosting functions.

A Breach Occurred. Now What?

In the unfortunate event of a data breach, the new law mandates that governed companies report incidents to DFS within 72 hours – even if the criminal attempt was unsuccessful.

Success is not the only measure of a cyber-attack's impact. The severity of the breach must be assessed to ascertain how likely it is to impact operations – and how badly.

DFS makes it is easy to report incidents: Simply access their website and click on the orange highlighted icon near the top of the page.

The law also makes it easy for non-exempt companies to access the information they need to file by requiring them to create and maintain the records of audit trails for at least three years.

When properly implemented, an audit trail is an immutable record that can help companies pinpoint the root cause of a hack, discover the extent of the damage, and identify vulnerabilities that need to be addressed.

Audit trails also have a deterrent effect on malicious users who realize every move within a system is tracked. When they are monitored in real-time, they can even combat cybercrime by quickly detecting unusual activity that might indicate user negligence, snooping, compromised credentials, or malicious intent.

Security issues identified in real time can be contained quickly – preventing a full-blown breach. While audit trails are only a requirement for non-exempt companies covered by New York's new law, they are considered best cybersecurity practices for all businesses.

How To Get Compliant While Fighting Cybercrime

Most businesses lack the expertise or manpower to meet the robust requirements of NYCRR 500. Instead, many are turning to cybersecurity experts like Motiva to help them protect confidential information and achieve compliance.

Our team remain vigilantly up to date on the constantly-changing threats created by cybercriminals. We have the expertise and tools to detect a wider range of attacks than in-house employees without the time or training to discover every possible breach.

Remember, it only takes one successful attack to cost financial companies large amounts of money and damage your credibility.

The needs of every business are unique, so we offers several tiers of customized service plans to help companies meet the mandates of the law. They range from turn-key outsourcing to self-serve plans that provide critical support to existing IT departments in businesses with a limited exemption.

We will do as much of the heavy lifting as companies want, including risk assessments, cyber and business policy templates, employee training, incident response plans, technology solutions, reporting to DFS, and more.

At the same time, we also safeguard your organization from advanced malware attacks, exploits, drive-bys, script-based attacks, and other dangers.

The idea of giving a third party access to critical corporate applications and sensitive data can be uncomfortable at first, but companies quickly understand that reputable cybersecurity partners are a much better defense against determined hackers than basic antivirus software or an IT staff with divided capabilities.

Outsourcing also can save companies money: Engaging a provider costs significantly less than hiring, training, and buying specific equipment for in-house employees. It also ensures around-the-clock access to experienced security professionals.

New York's new cybersecurity compliance mandates are bold, but they are not too difficult or expensive to achieve. A qualified cybersecurity provider can make these needed changes seamlessly for any business or organization.

Many of the requirements were already considered to be the gold standard for protecting sensitive data.

Talk to a trusted cybersecurity provider about the mandates of 23 NYCRR 500

We Have Deep Expertise in How Small to Medium Size Insurance Brokers Operate their businesses. We SPECIALIZE in IT services for small and mid-sized Insurance Brokers in the Long Island area. AMS – Applied Epic – HawkSoft . To name a few of the Agency Management Software that all of our Engineers are proficient with, so when you are calling because of your "accord form isn't working". We know exactly what you mean by it.

www.dfscompliance.com

(646) 374-1820

motiva