GLOBALCYBER CONSULTANTS

ARE YOU PREPARED FOR NEW YORK'S NEW CYBERSECURITY REGULATION?

The New York Department of Financial Services (NYDFS) recently released new cybersecurity regulations directly impacting all entities regulated by the NYDFS

The New York DFS Cybersecurity Regulation

The New York Department of Financial Services (NYDFS) new sweeping cybersecurity regulations went into effect March 1, 2017, which will directly impact all entities regulated by the NYDFS and inevitably affect compliance programs at financial institutions nationwide. New York Governor Andrew Cuomo announced the first-in-nation cybersecurity regulation to protect New York's financial services industry and consumers from the ever-growing threat of cyber attacks.

> ***"New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks," Governor Cuomo said. "These strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes."***

Regardless of whether an entity is headquartered in New York, the regulation extends to apply to all entities licensed by the NYDFS with limited exceptions for companies that have fewer than ten employees or less than $5,000,000 in Revenues. The comprehensive requirements of the regulation will not only significantly impact licensed entities by requiring enhanced policies and procedures to ensure compliance, but also many of their third party service and application providers. In summary, the rules will require industry standard best practices for cybersecurity programs and require firms to:

- Develop a cybersecurity program
- Assign a Chief Information Security Officer to oversee the program
- Conduct annual penetration testing and bi-annual vulnerability assessments
- Maintain an audit trail of activity
- Limit access privileges to information systems
- Develop written procedures and guidelines around application security
- Conduct periodic risk assessments to test and improve the cybersecurity program
- Provide awareness training and intelligence to personnel
- Develop third-party service provider policies that call for:
    - Cybersecurity risk assessments
    - Due diligence processes and evaluation criteria
    - Periodic assessments
- Implement multi-factor authentication for accessing information systems and nonpublic information
- Notify the DFS no later than 72 hours after a cyber event

TRADITIONAL SECURITY METHODS WILL LEAVE YOU EXPOSED

It used to be that compliance was just another word for a box to check off. Not any more. The new NYDFS Regulation has changed the regulatory landscape and is expected to set the framework for other states across the nation. Cyber Security is no longer an IT Department issue; it is now a matter of corporate governance with the growing awareness that cyber security has become a board level issue affecting all areas of an organizations operational, strategic and financial risk models. As firms continue to evolve and dependencies on third parties carrying essential business functions increase, attackers are becoming more sophisticated and targeting your partners, suppliers, and vendors through unwatched and often invisible entry points, giving them access to your network. As a result, the new regulation imposed by the NYDFS has included a central point of focus on your third parties' cyber security. ***This means the burden of proving the security of your third parties is your responsibility.***

With the increased reliance on third parties and the NYDFS regulatory requirements, old methods of managing third party risk are not enough and will leave your company exposed. Security questionnaires, although important, are labor intensive, often unstandardized and perhaps most importantly, only capture the firm's own, un-validated responses about their security posture at a static point in time. Continuous, standardized insight into a company's cyber risk and their supply chain is required to appropriately assess their security exposure at any given point in time. It is also critical to recognize that the traditional approach does not address new, important questions that need to be asked and answered to both comply with the regulation and effectively manage third party risk, including:

- How do you validate and verify the veracity of a self-questionnaire?
- How do you prioritize which third parties receive on-site visits? And at what intervals?
- Are you secure beyond the standards of 'reasonable' with a single point in time report to withstand negative regulatory interpretations?
- How do you gain operational command over your third party risk portfolio?
- Is the risk increasing or decreasing?
- Critical for executive leadership and meeting reporting requirements, can we prove that we've taken the necessary steps to assess, capture and remediate third party security risks?

As we continue to usher into the Digital Era, effective third party risk management requires a more holistic view of all the factors involved in digital security as it affects every aspect of a business. The pressure to keep up with constantly changing regulatory expectations have real and implied management costs. Similarly, perceptions of trust and reliability are necessary to keep customers loyal. There is a real and long-term business cost if you're found insecure or worse, that perceived insecurity leads to a data breach. This not only brings reputational risk, but the potential for class action and shareholder derivative lawsuits. The balancing act of keeping customers, regulators, and stockholders happy is difficult, but there are new tools and methods that allows information security managers to perform at an ideal pace with the needed actionable insights to quickly respond to security exposures.

HOW DO I GET AHEAD OF THE REGULATION?

Per the NYDFS Regulation, companies have 6 months to comply with the new regulations so time is of the essence! Starting on February 15, 2018, either a company's Chairman or a Senior Officer will be required to sign a statement that they have reviewed all of the applicable documents about their company and vendors that are needed to comply with the rule. Of course, in order to make that representation, the company actually has to have met the requirements and that is why leadership is required now.

For third party risk management, visibility into specific problem areas are the first task. You can get ahead of the regulation and manage your third parties with proactive diligence and remediation of issues by employing a collaborative approach. With Cyberfense, for the first time, your organization can take immediate action within your third party ecosystem. You can now see invisible regulatory risk in your network and within your third party networks. You can immediately see high-risk vendors and limit your exposure from day 1, while also ensuring continuous compliance with ongoing insight into your vendors' cyber risk. Within our platform, our security ratings provide actionable information and functional capabilities through continuous risk monitoring, offering organizations risk-critical information for any number of third-parties and on-demand security ratings through patented, non-intrusive assessment methods. This allows users to have a complete and comprehensive view of their third-party ecosystem from a risk-first perspective. Utilizing Cyberfense, your organization can view, benchmark, report, and collaborate on security risks to comply with the NYDFS Requirements by:

- Mapping security issues to the NYDFS Regulations and industry standards.
- Prioritizing which vendors need immediate remediation and on-site security audits based on their assessment.
- Isolating the partners that have risky assessments easily and rapidly without waiting weeks or months for accurate security risk feedback.
- Benchmarking your industry's security posture and compare against your competition to track security risk maturity in a more granular way.
- Gaining control of third party risk by improving time to remediation from weeks to days.

Our security intelligence platform, founded by two former CISOs and refined by on-staff whitehat security researchers and data scientists, transforms security data into action. Because the intelligence continuously captures new security information, organizations can confidently use the platform, set automated alerts, and always know when a scoring change occurs.

Organization's subject to the NYDFS Regulation can ensure third party vendor compliance utilizing the Cyberfense platform for immediate insight into vendor security risks and the actionable insights required to quickly remediate and take appropriate action.

About Global Cyber Consultants

At the forefront of digital innovation, Global Cyber Consultants works with worldwide organizations to ensure their assets are best protected while driving innovative change and operational efficiencies to secure sustained success and accelerated growth. With recognized industry expertise across insurance, technology, cybersecurity and finance/strategy, we ensure our clients they have industry leading resources and the intellectual capital required to maintain a competitive advantage within their own operating environment and the ever-changing business landscape.

At Global Cyber Consultants, we have created a standardized assessment that automates the manual processes of traditional risk assessments and allows companies to automate and streamline the IT and Vendor audit process by mapping to several security standards, such as NIST, ISO, HIPPA, PCI and the NY DFS Regulation, through one assessment. In responding to market needs, our platform also continuous insight into a company's cyber risk and their particular exposures, and what steps and the appropriate solutions that should be taken and implemented to better secure themselves with actionable insights and become "cyber competitive."