Automating the Risk Management of Third-Party Vendors Can Help Comply with NYDFS Part 500

NYDFS Cybersecurity Requirements for Financial Services Organizations Sets New Standards for third-party service providers

Published on December 4, 2017

Kimberly Carlos | Follow
Director of Cybersecurity Prod...

Automating the Risk Management of Third-Party Vendors Can Help Financial Service Organizations Comply with The New York State Department of Financial Services NYCRR 500.

New York State's Department of Financial Services *Cybersecurity Requirements for Financial Services Companies* (NYDFS Part 500) is setting rigorous new standards for information security. The requirements become effective in phases through 2019, and the financial services industry needs to be prepared.

One of the most challenging requirements is section 500.11 Third-Party Service Provider Security Policy. This section requires written risk-based policies and procedures designed to ensure security of information systems and non-public information accessible to or held by third party service providers (TPSP). Entities chartered or covered by DFS are required to provide an annual certification they meet requirements, signed by a senior officer or the company's board of directors with the first certification due February 15, 2018. To comply, financial service companies will need to show:

- Identification and risk assessment of TPSPs;
- Minimum cybersecurity practices to be met by TPSPs;
- Due diligence used to evaluate practices of TPSPs; and
- Periodic risk based assessments of TPSP.

Under this regulation, financial service organizations must have policies and procedures that include review and approval of the TPSP's own policies and procedures for access controls, including:

- Use of multi-factor authentication;
- Procedures for encryption;
- Notice requirements imposed on provider in event of a cyber event; and
- Representations and warranties provided by TPSP relating to the protection of information systems and non-public information.

With extensive and ever evolving regulation requirements, emerging innovative technologies, business pressures for acceleration, privacy issues and escalating cyber-attacks, it is easy to overlook the root of all these issues, risk management. As data breaches and cyber-attacks have become commonplace in the financial services industry, it is clearer than ever that being compliant doesn't always equate to being secure.

Many systems were not built with data security as the primary function and adding new technologies to reap the enhancement benefits can leave vulnerabilities for hackers to exploit. The market is swimming with innovative threat defense tools such as advanced endpoint protection, UTM firewalls, SIEMs, etc. But to effectively reduce risk to tolerable levels and to understand which areas need more investment of time or budget, companies must have a panoramic view of risk that takes into account all vectors of threats and impacts that can disrupt business.

SAI Global's Digital Risk Management solution for IT Vendor Risk Management can help financial service organizations with:

- Profiling, assessing, rating and remediating third-party and vendor risks
- Managing cybersecurity risks, threats, controls and countermeasures
- Managing compliance programs with regulations such as PCI, FFIEC, SOX, ISO 27000 Family, Center for Internet Security – CIS, 23 NYCRR 500, NIST Cybersecurity, 800-53, and 800-171
- Managing vulnerability assessments, analyses, and remediation processes
- Connecting IT risks with enterprise and operational risk management programs
- Controlling action plans and findings from internal audit
- Visualizing the relationships between digital assets, business processes, and risks
- Understanding what risk mitigation activities will be more efficient

To learn more about how SAI Global can help you comply with NYDFS Part 500, click below to connect with one of our digital risk advisers.

Speak with a Risk Advisor

#SAIGlobal

Kimberly Carlos
Director of Cybersecurity Prod...

Follow

0 comments

Sign in to leave your comment

More from Kimberly Carlos 8 articles

4 Best Practices For Third-Party...
February 23, 2018

Webinar: How to Simplify Your IT Vendor Risk...
November 14, 2017

Webinar Replay: Prevent a Ransomware...
August 30, 2016