TeamOne.Support

Military Grade Support * Because it IS a war out there.

Understanding NYDFS Cybersecurity Regulation Compliance for SaaS Providers

As of November 1, 2024, the New York Department of Financial Services (NYDFS) has implemented updated cybersecurity regulations under 23 NYCRR 500, imposing stringent requirements for financial institutions, including insurance companies. While SaaS providers and software companies are not directly regulated by NYDFS, they often play a critical role as Third-Party Service Providers (TPSPs) to these regulated entities. This whitepaper will outline the implications of NYDFS regulations for SaaS providers and offer guidance on how to align with these regulatory requirements.

Compliance Requirements for Third-Party Service Providers

Under NYDFS regulations, entities regulated by the NYDFS must ensure that any Third-Party Service Providers (TPSPs) that have access to nonpublic information comply with cybersecurity standards to protect this data. For SaaS providers working with regulated entities, the following aspects are essential for alignment:

Key Compliance Aspects

1. **Risk Assessment:** NYDFS requires that regulated entities perform a risk assessment for all TPSPs, identifying potential risks to nonpublic information.
2. **Access Controls:** SaaS providers should ensure strong access control measures, including multi-factor authentication and access restrictions based on the principle of least privilege.
3. **Encryption:** TPSPs must ensure encryption for nonpublic information, both in transit and at rest, to meet NYDFS standards.
4. **Incident Response and Notification:** SaaS providers should establish and communicate a response plan for any data breaches or cybersecurity incidents that impact their clients, including an obligation to notify clients promptly.

Contractual Obligations for SaaS Providers

NYDFS regulations require that covered entities include specific cybersecurity provisions in their contracts with TPSPs. SaaS providers should be prepared to meet these obligations in agreements with their clients, as follows:

1. **Access Control Policies:** Outline policies for secure access, requiring multi-factor authentication and defining access based on roles.
2. **Data Encryption Standards:** Specify protocols for data encryption at rest and in transit.
3. **Cybersecurity Event Notification:** Define a process for promptly notifying clients in the event of a security incident.

4. **Audit and Compliance Reports:** Agree to periodic assessments, audits, and provide relevant compliance reports as needed.

Practical Steps for SaaS Providers to Align with NYDFS Regulations

To ensure alignment with NYDFS regulations, SaaS providers should take proactive measures to address potential security gaps. Here are recommended steps for maintaining compliance:

1. **Conduct a Self-Assessment:** Review your current security policies and identify any gaps relative to NYDFS requirements.
2. **Strengthen Access Controls:** Implement multi-factor authentication and access restrictions to enforce least privilege access.
3. **Implement Data Encryption:** Use encryption for sensitive data, covering both in transit and at rest.
4. **Develop an Incident Response Plan:** Create and document an incident response plan that aligns with client expectations.
5. **Enhance Third-Party Risk Management:** Ensure that all subcontractors or downstream service providers also meet the necessary security standards.

Conclusion

While SaaS providers and software companies may not be directly regulated under NYDFS, their involvement with regulated entities as Third-Party Service Providers requires strict adherence to cybersecurity standards. By aligning with NYDFS requirements, SaaS providers can protect client data, reduce risk exposure, and enhance trust with clients in the financial services sector.

Services Provided by Security Privateers / TeamOne.Support

Security Privateers, led by Michael Scheidell, offers specialized services to assist SaaS providers in aligning with NYDFS cybersecurity regulations. Their expertise includes conducting comprehensive IT risk assessments, developing and updating information security and privacy policies, and providing guidance on regulatory compliance issues such as HIPAA, SOX, and FISMA. Additionally, they offer Virtual Chief Information Security Officer (vCISO) services, where Michael Scheidell, a certified security professional with extensive experience, can act as your named CISO. These services are designed to ensure that your organization meets the stringent requirements set forth by NYDFS, thereby safeguarding your operations and client data

TeamOne.Support offers a comprehensive suite of managed IT services tailored to meet the diverse needs of businesses, including those in the financial sector. Their services include:

- Technical Support: Providing responsive assistance to address and resolve IT issues promptly.
- Backup & Recovery: Implementing robust solutions to ensure data integrity and availability.
- Cybersecurity: Offering proactive measures to protect against cyber threats.
- Regulatory Compliance: Assisting businesses in adhering to industry-specific regulations.
- Client Access Portal: Providing a secure platform for clients to access services and support.

These offerings are designed to help organizations maintain a secure and efficient IT environment, ensuring compliance with relevant regulations.