Proposed Legislation

Drafted under the auspices of the Small Biz Thoughts Technology Community

www.smallbizthoughts.org

For more information, contact: Karl W. Palachuk, karlp@smallbizthoughts.org.

Note: "The [Appropriate Agency]" in this draft legislation should be replaced by the state police, cyber crimes task force, or whoever is the most appropriate agency in the state.

IT Service Provider Registration and Compliance Act

AN ACT of the _____ Legislature relative to registration with the Secretary of State by IT service providers and managed service providers; to provide requirements for doing business; to provide for definitions; to provide for time limitations on the reporting of cyber incidents; to provide for limitations on liability; and to provide for related matters.

Be it enacted by the Legislature of the State of _____

_____, [appropriate statute code] is hereby enacted to read as follows:

1. IT Service providers and managed service providers

A. The purposes of this Chapter are:

(1) To create a registration for IT service providers and managed service providers doing business in this state.

(2) To provide access for the general public to obtain information on IT service providers and managed service providers.

(3) To require IT service providers and managed service providers to report cyber security incidents and the payment of cyber security-related ransom.

(4) To define limits of liability related to cyber security and IT services

B. Definitions

As used in this Chapter, the following words and phrases shall be defined as follows:

(1) "Cyber security incident" means the compromise of the security, confidentiality, or integrity of computerized data due to the exfiltration, modification, or deletion that results in the unauthorized acquisition of and access to information maintained by a client of an IT service provider or managed service provider, as defined in this Chapter.

(2) "Cyber security-related ransom" means a type of malware that encrypts or locks valuable digital files and demands a ransom to release the files.

(3) The [Appropriate Agency] means _____.

(4) “IT Service Provider” means any individual, sole proprietor, partnership, corporation, limited liability company, or any similar entity or combination of entities that provides technology consulting services on an as-needed or hourly basis to companies, not-for-profit organizations, or public agencies at the state or local level in the state of _____ _____.

(5) "Managed Service Provider" means any individual, sole proprietor, partnership, corporation, limited liability company, or any similar entity or combination of entities that manages and maintains the information technology infrastructure or end-user systems on an ongoing basis to companies, not-for-profit organizations, or public agencies at the state or local level in the state of _____.

(6) “Provider” means either an IT service provider or managed service provider, as defined above.

(7) “Client” means any company or individual that engages the services of a provider.

C. Requirements for doing business

(1) A provider shall not provide IT related services in this state unless the provider has registered with the Secretary of State and remains in good standing.

(2) Beginning _____[Date]_____, each provider that offers IT related services in this state shall file an application for initial registration with the Secretary of State consisting of the provider's name, address, telephone number, contact person, designation of a person in this state for service of process, and provide a listing of all officers, all directors, and all owners of ten percent or more of the provider. Additionally, the provider shall file a copy of its basic organizational documents, including but not limited to articles of incorporation, articles of organization, articles of association, or partnership agreement.

(3) The Secretary of State may charge a filing fee to maintain related records, not to exceed one hundred dollars ($100.00) for each filing period.

(4) A registration shall be effective for thirty-six months, unless the registration is denied or revoked. Sixty days prior to the expiration of a registration, a provider shall submit a renewal application on a form or web site prescribed by the Secretary of State.

(5) The Secretary of State shall maintain a publicly-searchable database of all registered providers along with the beginning and ending dates of their registration, and all important information from the provider’s application, and information related to cyber security incidents and cyber security-related ransom payments as defined in this Chapter.

(6) Each registrant shall notify the Secretary of State of any material change in the registration information no later than sixty days after the effective date of such change.

2. Contracts between Providers and Clients

A. Contract Requirements

(1) Clients who engage a provider for services totaling less than five thousand dollars ($5,000.00) in a calendar year are not required to sign a contract for services. Clients who do not sign a contract for services shall not hold any provider liable for errors or omissions in an amount greater than the total dollar amount paid to provider in the previous twelve months.

(2) Clients who engage a provider for services totaling five thousand dollars ($5,000.00) or more in a calendar year shall sign a contract for services that is consistent with this Chapter and explicitly incorporates the provisions of this Chapter.

(3) Providers are required to inform prospective clients of the requirements of this Section.

B. Backup and Maintenance Minimum Requirements

(1) Any client who engages a provider for services and signs contract or agreement for services shall agree to pay for provider to create, maintain, and test data backups for all critical client data and IT services, except as described in this Section.

(2) If client chooses to not pay for provider to create, maintain, and test data backups, client shall sign a waiver releasing provider of liability under this Chapter. Any client who chooses not to engage provider to create, maintain, and test data backups, shall not hold provider liable for errors or omissions related to any cyber security incident or cyber security-related ransom during the period of their contract.

(3) Provider shall include in all contracts the creation, maintenance, and testing of data backups for all critical client data and IT services.

(4) Provider shall include in all contracts the maintenance and patching of all software and operating systems defined in the client between client and provider.

C. Notification of cyber incidents and payment of cyber ransoms

(1) To the extent a provider has knowledge of a cyber incident that impacts a client, the provider shall notify the [Appropriate Agency] of the cyber incident within sixteen business hours of discovery of the incident. The [Appropriate Agency] shall transmit this information to the Secretary of State within twenty-four hours.

(2) If a provider is aware of a cyber incident that impacts client and the provider or client makes a payment of ransom, to the extent the provider has actual knowledge of the payment, the provider shall report the payment of the ransom to the [Appropriate Agency] within ten calendar days of the payment. The [Appropriate Agency] shall transmit this information to the Secretary of State within twenty-four hours.

(3) A provider who submits a notification pursuant to this Section shall include in the notification the name of the client.

(4) Providers shall include the requirements of this Section in all contracts with clients. Both providers and clients shall be required to comply with the provisions of this Section to the extent the contract between the provider and the client explicitly incorporates the provisions of this Chapter.