It’s All About The Data

(Could we a little more specific?)

A COUPLE OF THINGS FIRST:

The Primary objective of data classification schemes is to formalize and strategize the process of contractually securing data based upon assigned levels importance and sensitivity (what a boring line but oh so true)

ALSO – Data classification is used to provide contractual language regarding mechanisms for storing, processing, and transferring data

DATA VALUE – can this be quantified in the contract?

Also addresses contractually how data is removed from a system and destroyed

This gets forgotten all the time in the real world and is the root of many time consuming incidents/lawsuits!

TO THE POINT

The number one benefit is that during the data classification process, the conversations alone impel the organization to identify those assets that are the most critical and valuable to the organization – INCLUDING ADDING THE CONTRACTS DEPARTMENT TO THE CONVERSATION

Contractually, should various data types be identified, particularly if of a sensitive nature?

Helps with managing risk as well as we consider contract language

Demonstrates the entity's commitment to protecting valuable resources and assets which helps with contract audits

Criteria by which data is classified: (so what does this have to do with Contracts?)

GOVERNANCE – HOW? BY COMMITTEE = IT/Contracts/Legal/Procurement

- Usefulness
- timeliness of the data
- value or cost of the data
- maturity or age of the data
- Lifetime – when does it expire
- National security implications
- Maintenance and monitoring of the data
- Association with personnel
- Storage

That word that should never be spoken (BUT SOMETIMES……)

What language was in the contract that talked about breach notification between us and our vendor/client, subcontractor etc.?

What regulations & statutes must your contracts contain reference to?

What reporting notifications must be stipulated?

- EXAMPLE

- In the event of a breach and/or security incident relative to the firm's data or work product, as discovered by the contractor, notification to the firm will occur within 24 hours to the Office of the CISO/General Counsel by telephone and e-mail. The contractor agrees to cooperate fully relative to inquiries regarding information security incidents and make available any and all records pertaining to such matters.

EXAMPLES/TEMPLATES

- “It is to be noted that contractor will follow the firm’s processes, procedures, and policies for all information security controls.”

- “It is understood that not all requests for system/data access might be possible due to internal policies and contractual stipulation with customers.”

- “In the event of a breach and/or security incident relative to the firm’s data or work product, as discovered by the contractor, notification to the firm will occur within 24 hours to the Office of the CISO by telephone and e-mail. The contractor agrees to cooperate fully relative to inquiries regarding information security incidents and make available any and all records pertaining to such matters. Contractor agrees at all times to provide, maintain and support its deliverable application/software/product and subsequent updates, upgrades, and bug fixes such that the Software is, and remains secure from vulnerabilities.”

EXAMPLES/TEMPLATES - CONTINUED

- “Contractor agrees to preserve the confidentiality, integrity and accessibility of the firm’s data with the same administrative, technical and physical measures that conform to generally recognized industry standards and best practices that the contractor applies to its own processing environment. Maintenance of a secure processing environment includes but is not limited to the timely application of patches, fixes and updates to operating systems and applications as provided by vendor or open source support.”

- “Relative to firm’s data currently in, and for data that will be, under the control of the contractor’s personnel/contractors, the contractor agrees to encrypt such data in conformance with industry best practices and standards.”

Place of performance: (you might add this if it is required by your company)

“It is to be noted that all services will be performed at the firm’s site(s) located at : wherever”

WHEN SHOULD ALL THIS HAPPEN?

At what point do the contracting officers consult with the information security office to obtain protection language to insert into the contract?

Or even vet the customer/vendor/contractor regarding their own cyber hygiene?

What compliance regulations then drive contract stipulations?

- Federal, Military/DoD, State, IRS, HHS, SEC, etc.

SYSTEM AND CODE DEVELOPMENT

If the contract calls for application/code development by either party, how do the contracting officers incorporate protections that protect the enterprise?

Where in the contract is the timeframe detailed regarding cyber? (vulnerability testing, code scanning, etc.) Breach notification stipulations – what do those timeframes look like and what federal/state mandates drive those timelines?

CLOUD UTILIZATION & CONTRACT NECESSITIES

ALL YOU REALLY HAVE FOR PROTECTION REGARDING CLOUD USE IS CONTRACT LANGUAGE!

GOOD LUCK GETTING AMAZON OR MICROSOFT TO CHANGE THEIR CONTRACTING LANGUAGE BUT ???

WITH OTHER PUBLIC/PRIVATE CLOUD PROVIDORS, MORE FLEXIBILITY

CLOUD HAS EVOLVED INTO ITS OWN CYBER SILO WITH MANY TENTACLES

Q U E S T I O N S ?