Privacy Prerequisites

During the pre-internet days the control, monitoring, and accountability regarding sensitive federal, military, or corporate intellectual property was a tangible physical activity where hidden documents or other recognizable media could be uncovered simply by controlling people and physical facilities.

The majority of our federal and state laws were architected around physical property to preserve ownership and enable the owner to control privacy.

Pop culture explored those behaviors in numerous movies where nefarious state-actors would infiltrate a building to capture photographic images or out-right remove file folders and paper documents.

In this generation data as property was recognized and this historical method of control was the prerequisite for early digital information control processes.

Digital Era Privacy

The rapid on-set of information digitization and transmission mediums offer significant value in terms of search, access, exchange, and repository management yet created a version of information exchange much less understood thereby leaving business owners to deal with a much less tangible risk interpretation. Subsequently digitized information invokes a much lower human perception of value where users often leave files, server access, or user credentials in a dangerously exposed position.

The current implementation of the internet protocol and subsequent architecture of systems and software imposes a multifaceted attack surface upon digital infrastructure. No longer is it acceptable to simply guard office access sites or monitor employees, this is out of your control.

Third-Party Risk Factors

The United States government and corporations are under continuous cyber-attack from nation state actors, organized criminal groups and others who routinely seek to undermine and steal from federal, state and municipal governments, private and public companies and individuals. The Department of Defense (DoD) is a target of attack and nefarious actors understand that the DoD and Prime contractors have strong protections in place so they focus attacks across the supply chain on smaller more vulnerable companies.

These risks are further compounded through the growth in Software as a Service (SaaS) and Cloud service offerings. The data your company creates is now processed, inventoried, and exposed to a myriad of physical hardware systems, facilities, and third-party employees across many states and foreign jurisdictions. This model further disconnects data as property controls. There is additional data control risk incurred as many of these SaaS and Cloud services have foreign national ownership and employees.

Despite efforts of the DoD to improve cybersecurity hygiene across the supply chain with cooperation through the development and education of National Institute of Standards & Technology (NIST) protocols such as NIST 800.171 there was no method to measure implementation and adherence. As of today, these have been primarily self-assessed and self-certify recommendations where in implementation has not achieved the desired results.

Cybersecurity Maturity Model Certification CMMC

The DoD has created the Cybersecurity Maturity Model Certification (CMMC) that applies to all organizations within the supply chain and enforces adherence across five levels of standards through audit by accredited compliance assessment organizations. The first phase of the compliance audit is estimated to begin in Q3 2020 and will be widely rolled out over the next few years. Companies that sell to the DoD, its primes and subcontractors will only be able to bid on contracts based on the level of certification they have achieved.

While this effort, currently only applies to DoD supply chain contractors, these cybersecurity hygiene practices offer a good common-sense strategy for any corporation, association, or agency across any industry. All business owners will benefit as this protocol combines employee training, corporate processes, and IT equipment requirements relevant to your level of privacy requirements. Market verticals such as financial services and medical will also adopt similar compliance regulations as they are seeking to standardize cybersecurity practices to protect their data as property from attack through the weakest link in their value-chain.

Compliance certification audits such as ISO are common practice in many industries where self-regulation is not effective and as such, we anticipate cybersecurity audits will also become commonplace. Similar to ISO qualification, Cybersecurity qualification will be a market advantage for the companies who publicly adhere to standards that protect the privacy of their customers and vendors while also ensuring business owner and shareholder value.

Enabling Corporate Compliance

Cybersecurity practices, IT system implementation and training will sound like an impossible task especially for the small and medium corporations with limited budget and workforce. Identifying and partnering with external parties will be critical in your success, protection, and certification.

When it comes to certification look to those DoD accredited service providers who know the CMMC protocol and more importantly how to interpret what is required for your particular type of business activities.

While dealing with the actual management of users, digital data, and auditability of your digital transactions between employee, customers, clients, and vendors Cicer One Technologies Inc offers a turn-key solution that is affordable and sustainable. The vast majority of subcontractor certification is estimated to be in the Level 1 to Level 3 range where the SCUTE product offers a simple compliance solution for any business. Cost effective and simple is critical especially for subcontractors where their DoD business may only be 10-40% of their total revenue.

SCUTE CMMC Compliance

CONTROLS	LEVEL 1	LEVEL 2	LEVEL 3
C001	🟩	🟩	⬜
C002	🟩	🟩	🟩
C003	⬜	🟩	🟩
C004	🟩	🟩	🟩
C005	⬜	⬜	🟩
C006	⬜	⬜	⬜
C007	⬜	🟩	🟩
C008	⬜	🟩	🟩
C009	⬜	⬜	🟩
C010	⬜	🟩	🟩
C011	⬜	🟩	🟩
C012	⬜	🟩	⬜
C013	⬜	🟩	⬜
C014	⬜	🟩	🟩
C015	🟩	🟩	🟩
C016	⬜	🟩	⬜
C017	⬜	🟩	⬜
C018	⬜	🟩	🟩
C019	⬜	🟩	⬜
C020	⬜	⬜	🟩
C021	⬜	🟩	🟩
C022	⬜	⬜	🟩
C023	⬜	🟩	🟩
C024	🟩	⬜	⬜
C025	⬜	⬜	🟩
C026	⬜	🟩	⬜
C027	⬜	🟩	⬜
C028	🟩	🟩	🟩
C029	⬜	🟩	🟩
C030	⬜	⬜	⬜
C031	⬜	🟩	🟩
C032	⬜	🟩	🟩
C033	⬜	⬜	⬜
C034	⬜	🟩	⬜
C035	⬜	🟩	🟩
C036	⬜	⬜	🟩
C037	⬜	⬜	🟩
C038	⬜	🟩	🟩
C039	🟩	⬜	🟩
C040	🟩	🟩	⬜

COMPLIANCE LEGEND	
COLOR	DESCRIPTION
🟩	SCUTE MEETS OR EXECEEDS REQUIREMENTS
⬜	THIS CONTROL IS NOT ENACTED AT THIS LEVEL

C041	🟩		
C042		🟩	🟩
C043			🟩

Cicer One Technologies Inc.

Cicer One Technologies Inc., a data privacy company. Cicer One's flagship hardware product SCUTE ushers in a new market segment of *Sealed System Technology* in IT that offers businesses a ransomware safe, globally accessible secure digital asset management and communications platform, complete with user management and full system audit reporting. (www.ciceronetech.com)

Sealed System Technology offers Embedded AI and Operational Behavior codified against Business Operations so Users and Systems are managed against generally accepted business practices. This device truly drives digital asset management automatically, to the benefit of the corporation. Digital information is managed and exchanged maintaining privacy and data as property ownership while removing all third parties or foreign exposure from the data transaction scheme Applying only general business skills you are able to easily organize and share files, manage and monitor users, protect intellectual property, and comply with privacy laws.