Are you CELF Aware?

As we here at Eigenspace continue our research into how to best prosecute the daunting task of proper Cybersecurity, we have continually run into challenges. The first is how to think about Cybersecurity…. We leverage the Cybersecurity Awareness and Resiliency (CAR) concept [Watchorn and Bishop, 2017]. Now that we have a philosophical outlook, we need more tactical approaches to this daunting challenge. We leverage the Cybersecurity Semantic Landscape Ontology and Taxonomy (CSLOT) [Watchorn and Bishop, 2017]. This comprehensive approach outlines all the major components of designing and executing a true Cybersecurity program. Our Cybersecurity "secret sauce" is our ability to understand all aspects of Cybersecurity Controls and how they are inter-related throughout the security lifecycle. In our discussions with others, we have discovered the first response is, "Wow. How do you do that?" Then we usually get some form of, "That is just overkill." That just makes us smile for two reasons, 1) when it comes to security, can you really be overkill? and 2) many times, we get, "We just don't have to do that." Now, if you truly understood our CSLOT and Level I and Level II, then you would know that we have incorporated and aligned MANY Cybersecurity statutes, laws, regulations, frameworks and guidance that are imposed on US based organizations. So, when someone reacts with "We just don't have to do that," we already know the answer, "yes you do, you are just not aware of that fact." This has high-lighted a need: how to explain the Cybersecurity Legislative impacts to an organization and the Cybersecurity EIgenWay Legislative Framework or CELF was born. Let's make you more CELF-Aware, shall we?

Our framework begins with a simple list of a few questions. This begins to "frame up" the legal picture for your organization. It begins with what continent is your organization based and which ones do you operate? Then, of course, what country(s) is your organization based?

These two questions begin the overarching umbrella of Cybersecurity and Privacy laws.

From here, we start iterating. Each law identified is scrutinized for Cybersecurity responsibilities, deliverables and applicability of other laws and references. Then, each of those identified references must also be scrutinized for responsibilities, deliverables and applicability of other laws and regulations. This multi-iteration process continues until there are no more new requirements, deliverables or further references.

If you reside in or do business with European Union and transmit, store or process Privacy information many laws apply to you, the least of which is the General Data Protection Requirements (GDPR).

Some examples in the US would be Federal Information Security Management Act of 2002 (FISMA), Cybersecurity Act of 2015, OMB regulations, Executive Orders, SEC mandates, etc.

Are you CELF Aware?

In the US, we have not only the list of Federal statutes, but we have state level as well. These are harder to track but are just as important. They range from breach notification to specific privacy requirements. These laws become very hard to navigate when an organization has offices nationwide. If a breach happens in a data center in California, for instance, the California state laws may apply.

The purpose of the CELF, is to increase Cybersecurity Awareness for your organization, specifically your Cybersecurity organizations. It brings to bear a framework that organizes the Cybersecurity teams for all Cybersecurity impacts from legal ramifications. This is NOT focused on replacing the value of an Organizational Attorney. The problem is sorting through all the compliance and Cybersecurity directives is becoming more and more difficult to read. We need our Cybersecurity professionals to increase their Awareness of the legal ramifications to elevate their CAR. This organizational awareness then frees up your Cybersecurity Attorneys to help track this framework's updates for each organization and represent the organization in court with support from the evidentiary based assessments provided by the Cybersecurity organization.

If you are interested in understanding how the CELF can help your organization, check us out on www.eigenspace.us.

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us