I'm confused as to the rigidity in Cybersecurity

As a former military service member, I have been trained to conduct realistic and comprehensive analysis for mission preparedness, performance, capabilities, execution, and resiliency. I have leveraged this background and experience to aid in my work in Cybersecurity from various roles and opportunities over my career in the National Security space. My experience and work ethics resulted in my selection to provide Chief Information Security Officer (CISO) services at a major fortune 500 organization for the last few years. One of my duties included monitoring changes in the Cybersecurity landscape and to anticipate the potential impacts on mission preparedness, performance, capabilities, execution, and resiliency. Starting in July 2017, I began to observe numerous changes to Federal guidelines, standards and regulations that began to give me pause from both a Cybersecurity Subject Matter Expert (SME) and CISO Practitioner point of views. This fundamental change was a holistic and systematic approach to revamping the concept of Cybersecurity to include resiliency as part of the decision-making process. I became concerned with the impacts that the changes may create, so I began to conduct investigations to determine how best to plan for the changes. These investigations uncovered such dramatic changes on the horizon that in December 2018, I started my own company to aid in better understanding these perceived issues that will occur during the change process to these new Federal guidelines, standards and regulations. My company is dedicated to clearly articulating the changes and helping any organization accelerate their knowledge, planning and compliance with this new Cybersecurity Landscape.

It is with this backdrop, that I continue to be amazed at the press regarding Cybersecurity. I also witness the Cybersecurity Industry and their marketing. This amazement is around continued pushing and refinement of the same old thing…. buy Cyber products, share threat intel, get to the cloud quickly, and embrace DevSecOps. Yet, when I or my company speak about the future that the US Government is positioning and our understanding of it, NOBODY listens. They don't understand or listen to what the USG is doing. They don't understand or listen to what my company is proposing to solve this challenge.

After extensive research, Eigenspace knows what the USG is trying to accomplish. We have done the analysis to understand every Cybersecurity Control and all their attributes. How it relates to Laws (Cybersecurity Eigenspace Legal Framework [CELF]), Regulations and Frameworks (Cybersecurity Landscape Ontology and Taxonomy [CSLOT]) and how to properly select Cybersecurity Controls (Cybersecurity Order of Operations Methodology [COoOM]). Additionally, the state of mind, organizational attitudes and organizational Cybersecurity

I'm confused as to the rigidity in Cybersecurity

workforce constructs are embodied by the Cybersecurity Awareness and Resiliency [CAR] concepts. These approaches, all documented products of Eigenspace, ensure you will be compliant with your contract, aligned with the intent of the USG, and build a scientific (not best practice or experiential) approach to Cybersecurity Control selection to ensure the maximum chance of staying secure.

So, for those who still believe that the same old thing is working, just look at the breaches that are being reported daily. It is not working. The reason is simple…. The workforce isn't getting the full job done. This could be for a multitude of reasons like, not enough resources, not enough time, not enough training, not enough skill, not enough patience with the business to do the right thing, not being patient and going too fast to meet business demands, etc. The Cybersecurity Industry isn't helping either. They are understandably selling their wares and services. BUT, they are all based on quick fixes and experience based on being hacked. In my observations, the constant successful hacks bear these truths. Given that, why doesn't anyone overcome the inertia to believe there is a better way? The USG has been outlining it for over a year. They are beginning to enforce it. Do you want to wait until the penalties arrive or damage done from being hacked? OR, do you want to start believing there can be a better way?

Yet, I'm further confused by the fact that the Cybersecurity Industry is crawling all over Eigenspace's website but nobody wants to engage with us. The top visitors to our website since January 1, 2018 are:

- Palo Alto Networks
- MITRE
- Amazon AWS
- Scitor.com (A SAIC company)

These are quite a list of influencers in Cybersecurity. They are mining our material to better understand the future of Cybersecurity, especially in the USG. Eigenspace stands ready to accelerate and help those organizations if they would like for us to engage with them. I also find it fascinating that our research and proposals are finding its way into the ecosystem without us. One of my last official vendor visits when I was CISO of SAIC was with a high-quality Software Defined Perimeter (SDP) company in November of 2017. My research partner and I presented our findings and proposed a network solution to address all the security controls required and the intent of the USG to protect networks including Controlled Unclassified Information (CUI) and

I'm confused as to the rigidity in Cybersecurity

Continuous Diagnostics and Monitoring (CDM). At the end of the presentation, we were told that our proposal was overkill. Nobody would build to this standard of protection. The government couldn't be really asking for all this. And, yet by March 2018, that same vendor proposed a new Zero-trust architecture based, at least in-part, on our proposal. So, it seems that Eigenspace's research has some validity.

If you want to get in front of these dramatic changes and understand the better way, please visit www.eigenspace.us.

For all CISOs and Information Security professionals, I strongly encourage you to ensure your organizations, writ-large, understand the Cybersecurity Workforce Framework, its companion Cybersecurity Framework and the security controls required from them to be compliant, have the comprehensive processes to be aware and agile to Cybersecurity change requirements, and keep your organizations out of trouble with the USG. Believe it or not, the Federal Government's laws, guidelines, standards, frameworks and regulations are NOT limited to the US Government Agencies and their contractors, it affects private companies in the US as well. (Oh yeah, we can help with that too…….).

For Additional Information Contact:

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