Case Study: A follow up to Cyber Rigidity

Two weeks ago, I wrote an article on how people and companies are being rigid when it comes to Cybersecurity (https://www.linkedin.com/pulse/im-confused-why-people-stubbornly-rigid-cybersecurity-aaron-bishop/). I received some feedback that sometimes ideas are so forward thinking that the average consumer can't make the "leap" in understanding how the new ideas apply. They suggested that I explain Eigenspace in a more "use case" type scenario to better bridge the gap in this lack of understanding. Being one who continually listens and learns, I am going to attempt to try something different and explain via a use case below…

Let's say you are a contractor to the Federal government. You are a publicly traded company. You have either a person or a team designated as the responsible party for your corporate compliance. This organization must handle everything from SOX compliance to DCAA and DCMA compliance (for those in the USG contractor business, you know about these organizations). Most publicly traded companies have an IT organization and a CIO running that organization. The CIO, most likely, is trying to help digitally transform the business and accelerating digital change with modern technologies like: Cloud, Cryptocurrency/BitCoin, DevSecOps, Virtualization, AI, IoT, etc. Most organizations have credit card purchases and managing them through their finance organization is key incurring a PCI-DSS requirement. Additionally, most of these companies are trying to have their organizations carry certifications as differentiators like COBIT, ISO and FedRAMP. There are many larger organizations that are doing business in the EU and have GDPR rules applying to them as well (or other countries' rules that the organization may be operating in). I would venture to say MOST of these organizations (but not all as I know things are slowly changing) have either an Information Security Manager or CISO in their IT organization. This entity (and their office) is responsible for their IT security compliance. Most large organizations also have some form of Risk Management Officer as well as a Chief Privacy Officer.

So, here we are. In a quick paragraph, we have identified NUMEROUS standards, guidelines, requirements and statutes (only at the International and Federal levels, not state level requirements and statutes). Most organizations have multiple people and/or organizations responsible for tracking, interpreting, implementing, assessing and managing the certification and assessments for all these standards, guidelines, regulations, requirements and statutes. In addition, they also must manage all 3rd party audits that are required as well. Quite a burden on any organization (and most probably wasteful as well).

Now to the individuals involved. The Cybersecurity Workforce Framework (CWF) requires that personnel who are working in a Cybersecurity role/job OR makes a Cybersecurity decision for the organization MUST be properly trained (and have evidence of that training when requested by the USG).

Case Study: A follow up to Cyber Rigidity

Finally, the Cybersecurity Landscape is constantly changing. Technologies are changing rapidly. Approaches and processes are changing at the speed of innovation. The Cybersecurity standards, guidelines, requirements and statutes at all levels (state, Federal, International, standards bodies, etc.) are changing almost daily.

With ALL this background and normal company organizational challenges, it is no wonder that there are many people who say they have experience and status quo "best practice" approaches. Yet, these do NOT work (risk management, best practices, dependency on certifications, ill-informed legal advice, etc.). This can be for a multitude of reasons…. But ultimately, it doesn't matter. Companies are getting breached at alarming rates….

So, how can Eigenspace help? Eigenspace has researched the fundamental building block of Cybersecurity, The Cybersecurity Control. A security control can be applied to any type of system, ICS, SCADA, IoT, OT, Information Systems, Cloud implementations, voting machines, etc. By understanding every attribute to the security control, we can begin to analyze against the remaining issues of Cybersecurity. Once complete with that analysis we can become predictive in nature rather than reactionary to best practice failures.

An example how this might help the above scenario would look like this….

Eigenspace has the Cybersecurity Awareness and Resiliency (CAR) Concept. The tenants of this outline how the organization should be organized and behave. Leveraging the CWF and the CAR puts the organization in a defensible posture that creates the highest percentage chance to make Cyber Aware and Resilient decisions going forward. How does an entity organize against ALL the stimulus against it (as outlined above)? That is where Eigenspace's Cybersecurity Landscape Ontology and Taxonomy (CSLOT) comes to the rescue. The purpose of this artifact is to illuminate, organize and track all the organization's responsibilities and tasks required for Cybersecurity and Compliance. Leveraging the Risk Management Framework (RMF), next, you would choose Security Controls. Here is where there is the biggest abuse of the RMF. Decision makers, Cybersecurity "SME"s, consultants and a myriad of others want to leverage "best practices" like CIS Critical 20, FedRAMP or CUI as the "what" to tell the organization the Security Controls need to be chosen. Sometimes the Cyber SMEs will choose others that they are familiar with. Sometimes the customer will choose a baseline via contract requirements. Eigenspace uses the Cybersecurity Order of Operations Methodology (COoOM) to be the litmus test to ensure that all Cybersecurity controls for each and every requirement are accounted for and properly selected. Eigenspace also recommends a new way to execute Accreditation and Authorization (A&A). By following our model (the *EigenWay*), an organization can focus their Cybersecurity efforts on risk analysis and true understanding of the Cybersecurity challenge, NOT paperwork. By using our methodology and tools, they will know they haven't missed anything. They will have the evidence required to be

Case Study: A follow up to Cyber Rigidity

compliant with all laws and documented all decisions from the beginning. They will have Awareness, Resiliency, Compliance and the BEST likelihood of a secure implementation by following this approach.

SO, how can an organization leverage this new scientific approach to Cybersecurity to their benefit? Follow this outline…

1. **Start with adopting the EigenWay.**
2. **Align organization per the EigenWay with the Cybersecurity Workforce Framework.**
3. **Focus energies on how to properly document the evidence of the Cybersecurity assessments and decisions.**
4. **Focus architecture and engineering to be Cyber Aware and Resilient (to include DevSecOps, Cloud, ICS, SCADA, etc.)**
5. **Take advantage of the EigenScore to show any auditor, insurance appraiser, or legal inquiry a non-human biased way to show progress against this approach.**

Eigenspace stands ready to help organizations on this journey.

For Additional Information Contact:

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