# Enterprise Risk

I have seen an increase in articles in media, conferences, and on this platform about the increase in Cyber Risk. More directly, these articles state Cyber Risk is now beginning to be characterized as an Enterprise Risk and should be tracked as such. I don't disagree with the importance this stance is trying to state. However, the moment we hear "Corporate" or "Enterprise" Risk, everybody's mental stance changes and they lose sight of Cybersecurity Awareness and Resiliency (CAR) [Watchorn and Bishop, 2017] for the organization. Typically, the organization then tries to apply existing Enterprise Risk methods, processes and organizational structure to apply to the newly added Cyber Risk. This violates CAR as well. These existing Risk personnel and methods do not work for Cybersecurity. CAR mandates the right people, with the right background and training, in the right role, in the right organizational construct, are empowered to make the right Cybersecurity decision for the organization to manage its regulatory responsibilities and identified Cyber Risk. It is not a committee decision. It is not a person in positional authority within the organization (regardless of traditional power, perceived importance, or by title) making business decisions priority over Cyber Risk decisions. Cybersecurity risk is not a risk that can be accepted or rationalized away, especially in the new regulatory landscape. Cybersecurity today requires an unprecedented level of Awareness that historical practitioners just do not have.

To prove my point, let's examine a simple comparison of two radically different Enterprise Risks. A) Manufacturing problems are creating delays causing the corporation to potentially miss its deadlines affecting revenues and B) security assessment of corporation systems states that the IT systems are NOT compliant or properly implementing all the required security controls. Now, how do most organizations handle Enterprise Risk once identified? They usually have some process to catalog the risk into a centralized Risk Register. Some organizations meet about it via committee or executive team. Some have a Chief Risk Officer. But, let's be honest, all of these processes are business processes that stem from Financial risk. So how does the person and/or committee for Enterprise Risk assess Cybersecurity Risk? Through the Financial risk lens? I posit that decisions made this way will ALWAYS be wrong. Who are in these committees or positions? Are they properly trained? Are they properly educated? Are they security practitioners? Then how can they make the Cybersecurity risk decision unilaterally? You wouldn't have an IT leader make corporate Financial decisions, so why would you have a financial decision maker decide on Cybersecurity issues?

What would be a better way to address Cybersecurity Risk at an Enterprise level? Organizations should have an individual designated as the Chief Information Security Officer (or equivalent). Please see my article https://www.linkedin.com/pulse/what-does-ciso-role-look-like-now-aaron-bishop/ for the Cybersecurity Workforce Framework (CWF) definition of that role. This individual should be outside the chain of command for the mission of the business (the mission should not be in a position to override the security of the systems supporting it) and report directly to the CEO or

# Enterprise Risk

Agency lead. That relationship allows the CISO to better understand the mission goals, the mission challenges, and have the awareness and empowerment to affect Cyber Resiliency throughout the organization.

I understand that there is a shortfall in Cyber personnel. I would even argue the shortfall is greater because many of the so-called or self-called Cyber experts out there don't meet the criteria to be qualified for the role according to the CWF.

One area I do see being asked to help or out-right manage Cyber risk is through the legal organization (either through the General Counsel, the Chief Risk Officer, Chief Privacy Officer or the newly coined Cyber Attorney). I think this on the surface is a great stop gap measure. I believe, however, that this is absolutely the wrong long-term approach. Attorneys and the General Counsel's office are there for legal review, legal advice, to represent the organization in legal proceedings and to be part of the governance oversight for the organization. You would NOT want that person to be involved in the decision making or in that chain of command. That would create, at the very least, a perceived conflict of interest. For example, you wouldn't expect an attorney to be the Human Resource hiring and firing official and then turn around and ask that person to represent the organization for advice in court proceedings based on that very decision? SO, why would we expect a Cyber Attorney to get in that same position? Additionally, the CWF clearly articulates the role of legal I the Cybersecurity arena.

Cybersecurity Workforce Framework outlines all Cybersecurity roles, including Cyber Legal Advisor. CWF role states:

Oversee and Govern (OV)→ Legal Advice and Advocacy (LGA)→ Cyber Legal Advisor → OV-LGA-001→ Provides legal advice and recommendations on relevant topics related to Cyber Law.

Notice in that description, there is nothing about managing, nothing about making Cyber decisions, nothing about executing any Cyber function (including Incident Response).

Another thing of note, the CWF also goes on to describe the education, experience, certifications, knowledge, skills, abilities and tasks required to be QUALIFIED to be in this role. CWF States:

> Work Role Name: Cyber Legal Advisor
> Work Role: ID OV-LGA-001
> Specialty Area: Legal Advice and Advocacy (LGA)
> Category: Oversee and Govern (OV)
> Work Role Description: Provides legal advice and recommendations on relevant topics related to cyber law.

# Enterprise Risk

Tasks: T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522
Knowledge: K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0261, K0262, K0267, K0312, K0316, K0341, K0615
Skills: S0356
Abilities A0046

That means, for Cybersecurity Awareness, the Cyber Legal Advisor MUST have more than a Juris Doctorate to his or her name or they are UNQUALIFIED in that role. Further, there is a separate role for Chief Privacy Officers that is NOT the same role. So, for those companies who designate a Chief Privacy Officer out of their legal departments, they should not be the same person for convenience unless they are qualified for both roles.

So, back to the concept of Enterprise Risk… There is a role that is defined, empowered and expected to perform the role of Senior Cybersecurity decision maker for the organization. We should NOT try to force feed something else into the process. We should not try to leverage existing financially based risk models in modern Cybersecurity risk. If we can remove these biases, implement CAR appropriately, I am confident any organization (with work) can take this model and move the organization into a Cybersecurity Aware and Resilient powerhouse.

For Additional Information Contact:

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