Abstract

The ever-changing landscape of Cybersecurity continues to provide opportunities and challenges for the Cybersecurity professional workforce. Since 2014, the increase in security standards, regulatory compliance and legal oversight has, in some instances, caused a form of Cybersecurity-paralysis. The mitigation of the paralysis resulted in the development of numerous Cybersecurity frameworks, theories, methods and industry best practices. This white paper provides a holistic approach to the Cybersecurity Fluid Dynamic Security theory (Watchorn & Bishop, 2016) and includes the Cybersecurity Awareness and Resiliency (CAR), Cybersecurity Semantic Landscape Ontology and Taxonomy (CSLOT), and Cybersecurity Order of Operations and Methodology (COoOM) concepts aligned to the discovery of the impact of human bias in Cybersecurity endeavors. The CAR provides the leadership dynamic, strategic goals and performance expectations. The CSLOT provides the mutable processing approach to the Cybersecurity paradigm, and the COoOM provides a systematic litmus test approach to provide the starting point for Cybersecurity. The resulting starting point from the COoOM then forces the justification process for evidentiary-analysis to determine the likelihood of a given security outcome that includes the fundamental "built in security by design" required to achieve security. Cybersecurity is the practice of providing a means or method to identify, protect, detect, respond and recover from a Cybersecurity event. The end-result of the comprehensive approach outlined in this white paper would be the ability to predict a Cybersecurity Black Swan Event by conducting analysis of the likelihood of a known security threat by security control.

In today’s Cybersecurity world, industry attempts to mitigate Cybersecurity risk through “best practices”, baselines, compliance, and leveraging self-declared “experts” and their knowledge. To understand the impact of these approaches and provide decision makers clarity in understanding their Cybersecurity decisions, an approach was created. This approach, known as Risk Management Framework (RMF), tries to establish an organized way to understand the risk to business/mission and how Cybersecurity risk applies to that business/mission. This paradigm has led to the misuse and outright abuse of the purpose of Risk Management Framework. What is the fundamental flaw to all these approaches and its encapsulating Risk Management Framework? Human bias.

How can we articulate this human bias? How can you gauge how impactful is this bias? Can we identify how this bias affects our Cybersecurity posture, or worse, the underlying organizational business/mission? An example of how these human factors throughout an organization’s decision cycles aggregate to unknown amounts of human bias that compromises Cybersecurity posture could be:

Organization X wants to execute a specific mission. The Executive Leadership is singularly focused on “execution” of that mission. Just by the mere vision statement “to execute” creates unwitting bias for its employees to focus only on execution as a priority. The Cybersecurity organization must choose what baselines they are responsible to meet for organizational compliance. Do they know why the other security controls are not selected and why? Does every single person making Cybersecurity decisions have the requisite background, experience, education, certification, Knowledge, Skills, Abilities and Tasks for their role per the NICE Cybersecurity Workforce Framework (NCWF)? Does the supply chain allow for proper vetting of the suppliers, subcontractors, and vendors? Will the acceptance of an item from your supply chain introduce risk you aren’t aware of but now affects your organization’s Cybersecurity posture? Are you using RMF to “accept the risk” to speed up or manage costs to execute the mission but by doing so, compromise your Cybersecurity posture? Has there been any decision in the development of ideas, process, solution, etc. that wittingly, unwittingly, knowingly or unknowingly compromise Cybersecurity posture? We can stop here in our example and see multiple places where these few decision points each introduce human bias to the ecosystem and each subsequent decision is made on flawed information aggregating to lower the security posture of the organization greatly (probably unknowingly). Therefore, we are seeing unprecedented compromise of just about every organization in the media today and we predict in the foreseeable future.

Cybersecurity today only addresses what a security engineer knows, auditors only audit what they know or their “compliance checklist” requires, industry believes compliance is all that is “required” and that should be enough without understanding the ramifications of their decisions. What would be better than status quo? We believe a Cybersecurity Data-Driven approach is the answer. So how can we set the stage for common vernacular and a unified approach?

The concept of Cybersecurity Awareness and Resiliency (CAR) has three specific elements, which must work together to provide a security posture required in the 21st century and beyond. According to Merriam-Webster (2017), CYBER is defined as “relating to, or involving computers or networks (such as the Internet) or within the cyber marketplace.” As posited by Merriam-Webster (2017), the Cybersecurity definitions both apply to this concept. Merriam-Webster (2017) defines AWARENESS as “the quality or state of being aware, knowledge and understanding that something is happening or exists.” As postulated by Merriam-Webster (2017), both Awareness definitions apply to this concept. Merriam-Webster (2017) defines RESILIENCE as “the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress or an ability to recover from or adjust to misfortune or change.” As claimed by Merriam-Webster (2017) the Resilience definitions do not apply to this concept.

MITRE (2017), defines resiliency as “cyber-attacks requires technical, procedural, and policy changes to the infrastructure, architecture, and enterprise operations.” CAR modifies the posited Merriam-Webster and the MITRE definitions to declare its definition, which is “the ability to predict, identify, protect, detect, respond, and recover known and unknown attack vectors wherever they may be found.” This includes the decision-making process of individual or groups that may affect or compromise security postures for an organization. The CAR ethos requires a litmus test that measures for the effect in the decision-making process by detecting the wittingly, unwittingly, knowing and unknowingly impact for ethical, moral, and legal characteristics for security. Thus, the character of security within the context of Cybersecurity reinforces the CAR concept by adherence to the morality in decision-making processes measured by the outcome for accountability and responsibility for a given frame of reference.

The ability to dynamically adjust leadership to adopt to this form of moral conscious will require a new type of Cybersecurity Executive Leader (CEL) and elevates the role of the Chief Information Security Officer (CISO) as a key contributing member of the Board of Directors (BoD) decision-making process (or any Key Decision Maker). The CISO should be supported by a team of subject matter experts, that provide the due diligence of emerging security standards, requirements, and technologies to achieve the primary goal of the CAR, which is to ensure moral, ethical and legal Cybersecurity decisions as a factor of honest authority and legal awareness. The CISO’s team should be independent to operational business decision-making processes and have an isolated budget that supports, defends and protects the security posture required in the data concentric 21st century and beyond. The CAR provides a conceptual idea needed in the ever-changing world of Cybersecurity that now includes the evidentiary requirements of transparency, accountability and responsibility for the protection of data provided by the customers, clients and employees for today and the future.

Once we all agree that an organization must adopt the tenets of CAR, then how do we begin to implement such an aspiration? We should remove human bias so that we do not create a situation where an organization (or its employee) wittingly or unwittingly, knowingly or unknowingly compromise Cybersecurity and, therefore, violates the CAR concepts. This means a scientific and logical approach, not one on individual knowledge, assumed or misunderstood risk, and ill-informed decisions. This scientific approach can be accomplished through careful analysis of security controls. If we dynamically map every security control against all known baselines, all known architectures, and all known attributes of each control, we can begin to understand the interactions between these controls. We can further understand that if you de-select a control, you now have the awareness of what other controls you have missed and/or compromised by that decision. You can understand the control’s relationships to Federal requirements, security baselines, and Cybersecurity workforce responsibilities down to the control level. And because this is a security control analysis, it applies to all forms of information management: Information Systems, Cloud Systems, On-premise systems, Integrated Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems and Internet of Things (IoT). This level of understanding is the only way to truly establish CAR in your organization. While having this detailed understanding begins to educate the organization, it isn’t very actionable. So how can we help organizations prepare for this modernized approach to achieve CAR? We use the Cybersecurity Landscape Ontology and Taxonomy (CSLOT).

The Cybersecurity Semantic Landscape Ontology and Taxonomy provides a structured approach to the dynamic needs of the Cybersecurity security concepts, theories, standards, and compliance issues facing the 21st century of consumers. The CSLOT provides this by deconstructing associated activities into logical processing objects to provide the highest level of pre-analysis required to develop a discrete understanding for a given Cybersecurity engagement to include technical and non-technical personnel within the Cybersecurity Workforce. The construction of the CSLOT requires both a semantic and taxonomy fusion capability to provide the required analysis steps and processes to achieve the desired outcome of Cybersecurity excellence. The ability to organize the specific activities of a given outcome requires that each be defined, structured and implemented with a measured outcome or vetting activity to deliver the evidence of proof. The approach defined within the CSLOT incorporates eight specific activities to provide a repeatable orientation perspective to the development identifying risks, standards, and provide a means, method and capability that are required to operate within a Cybersecurity environment.

Any organization has a strong commitment to the protection of is corporate identity, brand and intellectual property. The CSLOT provides an insight into our level of organization theory, thought, leadership and practical standards of implementation in establishing Cybersecurity excellence. The CSLOT provides an organizational approach to manage our commitment to our shareholders, clients, stakeholders, and employees on the importance of Cybersecurity Awareness and Resilience (CAR), a primary tenant of our dynamic security approach. We understand the importance of CAR and have defined our processes and offerings around a strategic commitment to Cybersecurity excellence. We understand the importance of providing the most qualified workforce, which includes the ability to train to understand the Cyber Security Decision Matrix (CSDM) and delineated within the Cybersecurity Workforce Framework (NCWF) and its alignment with all known federal, state and local standards to ensure that our evidence-based approach provides the required measure of known good to all parties involved.

The CSLOT has eight levels, which are provided below with descriptions of services for an approach to Cybersecurity excellence. Each level should be completed in its entirety prior to proceeding to the next level and each should have a training element associated with the knowledge requirements, job description and common task functions required for each level. A general description is provided below for an evidence approach to how the organization approaches the responsibility of CAR and Cybersecurity Excellence.

Level 1: Domain Awareness – provides for organizational awareness on how to conduct Cybersecurity Situational required activities.

> Information Technology Cybersecurity Conflict Divergence (ITCCD) – provides a Cybersecurity orientation of primary and specialized knowledge levels of a given activity. The need to understand how each Cybersecurity concept affects the landscape begins by defining who has what operational knowledge of the given task, problem or operation to determine the ability to measure the Cybersecurity cognizance contribution into the dynamic leadership management paradigm. The two areas of primary and specialized knowledge are further broken down to provide conceptual decision-making responsibilities and accountability activities.

Joint Architecture Reference Model (JARM) – provides the Department of Defense (DoD) approach to how both Cybersecurity and Operational concepts would provide for cross-supporting activities and engagement. The ITCCD and JARM can be blended together to provide the required security posture required for DoD clients.

Level 2: Cybersecurity Risk Compliance and Information Assurance (CRCIA) – Provides a centralized method to identify all known risks, compliance, information assurance and applicable frameworks to achieve a viable security posture. The CRCIA, incorporates the Cyber Security Framework (CSF), Risk Management Framework (RMF), Continuous Monitoring Framework (CMF), NICE Cybersecurity Workforce Framework (NCWF), Cybersecurity Resiliency Engineering Framework (CREF), Supply Chain Risk Management Framework (SCRMF), Policy Awareness Framework (PAF), Forensic Investigation Framework (FIF) into a unified analysis model to define, process and describe the organizational security Cybersecurity risk posture for clients.

Level 3: Cybersecurity Order of Operations and Methodology (COoOM) – provides a method for building the required security control baseline, that transcends human bias in security control selection to include analysis of the many varied states of a given security control. Additionally, the Federal Information System (FIS) and Non-Federal Information Systems (NFIS) analysis required for the different versions of the NIST SP 800-53 are defined to build a comprehensive security control baseline, which provides the highest level of security analysis required to achieve a known Cybersecurity Risk posture for our clients.

Level 4: Common Cybersecurity Threat Framework (CCTF) – provides a common means and method of how to standardize the language of Cybersecurity related activities and enables a consistent categorization of a threat. The four layers are 1) Stages, 2) Objectives, 3) Actions and 4) Indicators. The CCTF has several sub-processes, which enables the framework to define capabilities of defined targets and measure the outcomes of the attack profile. Each layer of analysis requires a defined prosecution of a given Cybersecurity threat to determine likelihood and the outcome of the process would define the validity of a Cybersecurity-attack vector for analysis by Level 5 of the model. This provides a simple, yet flexible, collaborative way of characterizing Cybersecurity activities that supports analysis for all levels of Cybersecurity.

Level 5: Cybersecurity Vulnerability Reporting Framework (CRVF) – provides a data fusion analysis capability to look at the landscape of Vulnerabilities into a single ontology and taxonomy to define the data structure for storing and conducting analysis for the validation of a Cybersecurity threat to determine likelihood of effect or consequence on an Information Systems that has been defined as mission critical. The CRVF leverages the Common Vulnerability and Exposure (CVE), National Vulnerability Database (NVD) and Vulnerability analysis provided by the National Institute of Standards and Technology (NIST) and the National Vulnerability Database (NVD) managed by the US CERT program to provide a unified analysis capability to determine the attack vector and common mitigation processes to resolve a known security issue.

The CVE, NVD and Vulnerabilities provide a unified framework for reporting, researching and conducting analysis of past, present and emerging Cybersecurity Vulnerabilities to achieve a dynamic means and method to determine analysis requirements for any information system. The ability to search each system dynamically offers the outcome of fusion analysis using common lexicon mapping to known security controls provided by the NIST SP 800-53 and keyword associated activities. Additionally, the collection of the history of a given security vulnerability provides richness for contextual analysis required for Cybersecurity Awareness and Resilience (CAR), a primary tenant of the CSLOT approach. This provides a measurement of a risk profile based on the likelihood of attack assigned to a known vector of attack.

Level 6: Cybersecurity Artifact Repository Framework (CARF) – A common repository of Cybersecurity related artifacts required to demonstrate the current, past and future continuous monitoring requirements for a given system. Common artifacts would include the following; however, could be expanded to demonstrate totalitarian documentation for a given system or systems: 1) Security Control Baseline (SCB), 2) System Security Plan (SSP), 3) Plan of Action and Milestone (POA&M), 4) Legal, 5) Risk Management Framework Profile (RMFP), and 6) Security Content Automation Protocol (SCAP).

Level 7: Cybersecurity Resiliency Review (CRR) – Provides a prescriptive analysis phase that defines the various elements of CAR with assessment for evidence and validation of reporting security standards to determine the maturity indication level (MIL) for a given information system. The CRR has 12 elements that work together to provide a binary analysis of the organizational information systems, which include: 1) Asset Management, 2) Controls Management, 3) Configuration and Change Management, 4) Vulnerability, 5) Incident Management, 6) Service Continuity Management, 7) Risk Management, 8) External Dependencies Management, 9) Training and Awareness, 10) Situational Awareness, 11) Goals and Questions, and 12) Maturity Indicator Level (MIL). The MIL has five levels, each of which defines the level of evidence provided by the organization to demonstrate the adherence to the described standards for CAR and CRR overview analysis can provide a measurement to provide a Risk Assessment Posture (RAP) score for Clients.

Level 8: Deep Analysis – The ability to blend the concepts of Artificial Intelligence (AI), Natural Language Processing (NLP) and Deep Package Analysis required the unification of various research disciplines into a common approach lexicon for Cybersecurity operationalization. The Cybersecurity Predictive Helix Analysis Capability (CPHAC) solution provides the ability to describe Cybersecurity relationships and document the potential impacts from several discrete perspectives to develop a derived security analysis. The CPHAC provides the backbone for analysis by building the required dynamic relationship and includes the organization structure analysis required to execute an organizational approach to CAR and the preceding seven levels of the CSLOT. Each of the eight layers work in unison to provide for the highest degree of measured Cybersecurity adherence and is the common lexicon for the organizational approach to internal best practices and the services offered to our clients.

The CPHAC is our premier as a service offering, which we use to help define, organize and discover the various Cybersecurity related activities to determine our unified approach to security. The CPHAC provides means, methods and capability for documenting dynamic and discrete relationships found in the Cybersecurity domain. It incorporates the ability to find hidden relationships between vendor products and security controls. The organizational structure provides a visualization of the required concepts needed to engage on any Cybersecurity activity to bring about the highest level of CAR and Cybersecurity excellence possible because of its defined method for security concepts mapping and use of dynamic risk calculations for a myriad of uses. Distinct analysis provides insight into fusion analysis, which then provides more analytic analysis requirements to discover the various states of CAR within a given CSLOT or specific level of CSLOT.

For example, the ability to align the impact for the OMB Circular A-130 to the NIST SP 800-53r5, including the documentation of the 24 different states of a given security control, and the roles and responsibilities for evidence and forensic analysis standards to ensure that any organization achieves the CAR goals and has the added ability to define the Cybersecurity Security Framework (CSF) elements that reinforce the needs for the US CERT Cybersecurity Resilience Review (CRR) tenants to provide the evidence to prove that we do what we say we are doing. All organizations should strive to achieve a “baked in security” approach that is the true standard by which all organizations should be measured by and we invested in the CPHAC to help make that our concentric circles of Cybersecurity edge offerings to provide the highest level of security. Our approach required taking a forensic analysis phase and overlay with a criminal investigation phase and blend the outcome together to achieve our end state of CAR and Cybersecurity excellence.

One of the most misunderstood levels of the CSLOT is Level 3, the Cybersecurity Order of Operations Methodology. This is the heart of how human bias can be removed. With the release of the SP 800-53 rev 5, NIST has de-emphasized the importance of the industry bedrock paradigm of confidentiality, integrity and availability. They have also de-emphasized baselines in favor of security control efficacy. What does this mean for FedRAMP and the like? **It is clear to us that baselines are nothing more than an approved selection of security controls by an accreditor at a singular point in time.** Understanding each control, its importance, its relation to the mission, its interdependency on other controls and its state as it relates to ALL these important attributes (legacy and new, like confidentiality, assurance, integrity, privacy, operational, technological, managerial, organizational, etc.) is the only legitimate approach going forward in Cybersecurity. The NIST SP 800-53rev5 creates states of each control that must be independently assessed to an evidentiary level and cross-checked for is different states' applicability before final adjudication of accreditation. Some example security control states in the SP 800-53rev5 and its associated documents that each control needs to be evaluated are: Required, Joint, Privacy, Assurance, Situationally Required, Discretionary, Organizational, OMB, DOJ and Withdrawn. To properly assess each control, each accreditor must see the evidence required for each assessment for each state for each control and its related controls. If this is true, then the proper way to build a System Security Plan (SSP) would be **start with ALL 912 Cybersecurity controls**. You would have to justify in your assessment evidence the de-selection of any control. This process of understanding the overall impact of a single control against all possible states is the basis for the COoOM.

To be clear, after executing your Cybersecurity approach via the CSLOT, the last level is the failsafe to understand if you introduced bias along the way. Eigenspace has spent energy researching Cybersecurity Controls to help expose where human bias was introduced into the Cybersecurity Ecosystem. The CPHAC leverages our Cybersecurity control fluid dynamic assessment of security controls. It allows a scientific review of all states of security controls and their relationship to every other control to ensure a comprehensive analysis is completed. This predictive analysis is the "Rosetta Key" to uncover human bias introduced into a Cybersecurity approach. We are pioneering a new science to how Cybersecurity should be prosecuted leveraging data-driven decisions to be successful rather than relying on chance with risk-based decisions.

If an organization wants to improve its Cybersecurity approach from a human biased, legacy paradigm and leap-frog to a modern scientific paradigm, then we believe you should begin with organizing for success with a Cybersecurity staff that aligns to the CAR. This dedicated and properly resourced staff are properly trained in alignment with the Cybersecurity Workforce

Framework. Ensure that the organization leverages the CSLOT to holistically affect the Cybersecurity process to ensure adherence to the principles of the CAR. Most importantly, the organization leverages the COoOM to decide scientifically, what security controls to choose while not succumbing to the temptation to "manage risk" by de-selecting security controls without understanding the impact.

We call this the entire new paradigm the ***EigenWay***.

For Additional Information Contact:

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