The new Accreditation and Authorization model of the future

I have been investigating and researching the state of cybersecurity diligently over the last two years. Through all my learning, I have concluded: In order to successfully prosecute REAL Cybersecurity, an organization must totally revamp their Accreditation and Authorization (A&A) approach. Let me elaborate…

Today, risk-based approaches dominate how organizations decide what to do for cybersecurity. We leverage some form of risk management (NIST RMF, ISO RMF, etc). Regardless of which risk approach an organization chooses, it is all based on risk decisions made by humans. Someone decides to do this or that or accept this risk and not that risk. BUT, the reason for the risk decision is based on many other influences within the person and NOT the science and fact of Cybersecurity (some examples of human influences: speed to market, mission imperatives, or worse, accept the risk because it is a cheaper alternative). Sometimes, the person who makes that decision isn't even known by leadership, yet it impacts the entire organization. Then we, as Cybersecurity practitioners, are pressured to accelerate the risk management process for the sake of expediency that is required by the business or mission. Then risk continues to be bent or ignored, or worse, "accepted", with no immediate or apparent ramifications of that decision. I've discussed my feelings before on misused RMF in previous posts. I even cited a movie, "*Deepwater Horizon,"* where supervisors/managers in the business chain of command make risk-based decisions without understanding the technical impacts that compromise another decision unknowingly to them. That then cascades to another decision point that again "cheats" the proper process or behavior for the sake of slight risk. But instead of inheriting a little risk with that one decision, they inherited the compounding risk of previous decisions as well, even if unintentionally, to disastrous effect. So, risk today is feeding the A&A process with flawed decisions.

Then there is compliance. Again, I've discussed how compliance is nothing, but a security state assessed by a particular auditor at a moment in time. It is not a real reflection of true security. How do we come up with security checklists and baseline compliance? Someone personally lists out "best practices" like SANS Critical Security Controls or some regulatory organization focused on some aspect puts a list together like NIST SP 800-171. This Controlled Unclassified Information protection guidance (NIST SP 800-171) is focused on the confidentiality of the data. What happened to other aspects of the data, like integrity, assurance and availability for example? Those controls that affect those modalities are included in the NIST SP 800-53 compendium of controls. But because not every single control applies to every single solution, there is a way in RMF to de-select controls. The biggest flaw in today's RMF process implementations is overuse or out-right abuse to remove controls for convenience rather than truly understanding the reason to de-select them. The NIST SP 800-53rev 5 introduces new states of organizational controls, assurance controls, privacy controls, etc. The NIST SP 800-53 (all revisions) addresses the concept of Management, Operational, and Technical controls. This forms not the COMPLETE focus of controls, but the BASICS of controls. There are many other facets to a Security Control, like enhancements

and supplemental guidance, etc. One shouldn't remove a control and never look back at that decision. I argue they should START with the entirety of the NIST 800-53 control set and justify from there what should be deselected with justification. Baselines were created to remember which security controls were arbitrarily chosen. It became a shortcut to get to approval for A&A. So, compliance today is a short cut to today's A&A process that is rife with flawed decisions.

If risk and compliance approaches today were so good and best practices were effective, then why is everyone getting compromised at alarming rates? The fact is the common dominator to this weakness across the risk management models, best practice approaches and compliance approaches is the lack of understanding the ENTIRE CYBERSECURITY SPECTRUM when making decisions. It must be without human bias. It must be scientific. It must be comprehensive. It must be understood. This is the main tenants of the Cybersecurity Awareness and Resiliency (CAR) Concept.

Deputy Secretary of Defense, Patrick Shanahan spoke on February 6, 2018 to a public crowd and effectively told the Defense Industrial Base that they need to change the way they are thinking about protecting data. He called out CEOs of companies that if they don't take Cybersecurity seriously the way DOD has outlined it, then they won't be doing business in the future with the Department of Defense. If everyone is using risk-based approaches, best practices and executing correctly, why would he have to make this statement? It is because status quo is not working. Everyone is getting hacked or has been hacked. This announcement creates more issues than just calling out the efficacy of security control selection, risk management or compliance programs. It assigns accountability. No more is this merely a security office problem. No more singular Designated Approval Authority decision to "go or no-go". The Deputy Secretary called out CEOs of companies. The NICE Cybersecurity Workforce Framework lays down very specific roles in the lifecycle of Cybersecurity. To be compliant with the intent of the US Government (USG), you must know WHO is making the Cybersecurity decisions and that they have the proper background, education, training and certifications to hold that position. Additionally, they will be held accountable along with the entire organization. You can't just fire a person as a scape-goat anymore. The organization will be held accountable as well.

Empowered by many laws and statutes, the US CERT is quickly preparing to provide not only continuous monitoring capabilities to USG systems, USG data (wherever it resides), USG Contractors (yes, the contractor's facilities and systems) and USG providers (all types, including cloud providers) but also forensic investigatory responsibilities. What does this mean? Per the contracts you sign with the USG, the US CERT will review, scan, and assess your organization to ensure you have standardized process, your documentation is correct, you are following ALL prescribed standards and are doing "what you said you would" to an evidentiary standard. BUT, if they find anything amiss, they are bound to turn the findings over to the FBI and US DOJ to be

assessed for violations of law and possibly prosecution. Taking risks and following historic best practices, just isn't good enough anymore to meet this high standard.

So, what does all this mean and how does it relate to A&A?

If an organization believes in this analysis and ascribes to the tenants of the CAR, then they need to be comprehensive in their approach from THE BEGINNING.

1. **The organization must begin by organizing themselves in alignment to the NICE Cybersecurity Workforce Framework. The reason for this first effort is any organization can't declare that the planning, control selection, decision authority and assessors of Cybersecurity can be done by unqualified personnel and still ascribe to the tenants of the CAR. Additionally, anyone who knowingly or unknowingly; wittingly or unwittingly makes a decision that affects the cybersecurity posture must be in the correct position to make the decision, be PROPERLY trained and can JUSTIFY the decision. If not, then it is a violation of the CAR, Cybersecurity and needs to be managed as an incident. This means that the CISO or DAA MUST NOT report to the mission or function head for segregation of duties and to prevent a decision being made in a conflict of interest. The Cybersecurity decision cannot be arbitrarily overridden and preserve CAR and Cybersecurity.**
2. **Next, the organization must create a rigorous training program. This isn't about a Security+ and CISSP. Those are important certifications, but it needs to include holistic training across the security paradigm. What role is the person in? What role in the hierarchy does the person reside? What decision authority in the org chart does the person possess? These questions drive training, education and certifications specific to their role. What vendor training is required in the performance of their duties? What are the mandatory training required depending on delivery methodology (on-prem, hybrid, cloud, etc.)? And most importantly, in Cybersecurity, this endeavor is never over but a constant requirement.**
3. **Next, the organization needs to have a comprehensive process to address Cybersecurity holistically. That means they need to follow the Cybersecurity Semantic Landscape Ontology and Taxonomy (CSLOT). This singular document provides a standardized model for assessors and investigators to measure cybersecurity against to ensure comprehensiveness.**
4. **If you follow a prescribed comprehensive method, then you need to justify your control selection through a rigorous process. The CSLOT, Level 3, provides such rigor: the Cybersecurity Order of Operations Methodology (COoOM). By identifying each control required for all states of each control and how it is used (including all enhancements, supplemental guidance, etc.), this then allows the team to focus on proper assessments, control by control, throughout the A&A process. That alignment of understanding is key to quality engineering and design for TRUE security.**
5. **Another aspect is the vendor selection process. Your vendor choices are building blocks to your solution. Do you have a rigorous supply chain management process? Does that process vet your suppliers both as an organization and their product? What controls does their product mitigate? How do you know? What assessment has been done to understand those claims? Does your vendor meet the regulatory environment your solution is targeted for? Is there an Open Source component to the product you are considering? If so, do you have a**

comprehensive process to vet Open Source components for EULA legalities, vulnerability inheritance, transfer rights, etc.?

6. **Yet another aspect is your development lifecycle. Does your development lifecycle follow the CAR tenants or not? Does the choice of speed remove Cybersecurity rigor? Are the developers and integrators properly trained in Cybersecurity? Again, if a person knowingly or unknowingly, wittingly or unwittingly makes a decision (in this case in development) that compromises Cybersecurity posture, they are to be held personally and corporately liable for any damages created because of that decision.**
7. **As part of the assessment process, the team should be thinking about evidentiary based collection of proof of assessment for each control and how it ties into continuous monitoring at an evidentiary based standard. Were the CAR tenants followed rigorously throughout the engineering and design process? This is important for the contractual and evidentiary responsibilities of the organization.**

While this seems a simple list of steps, it really is quite complex. This point drives home even further the absolute requirement to have a comprehensive process. BUT, if your A&A process begins, flows and ends this way, the adjudication of a system is completely binary and non-human biased. It is simple. Did the person selecting the controls have the proper background? Did they understand the environment the solution will be residing? Did they select the proper controls (not on a baseline but scientifically)? Did they understand the vendor selection impacts? Did they understand the solutions inherent vulnerabilities? Did they understand the attack vectors their solution presents? Have they properly documented and assessed each control of the solution to an evidentiary standard? Have they been third party assessed by the same methodology but different person's assessment to ensure there is nothing left to chance within reason. If the organization takes this A&A approach, then adjudication is a simple review of the process. There is no one person making a deadly mistake of "I will accept that risk" and not understand what impact to the organization was just done.

This approach presented is called the *EigenWay*. Leveraging the *EigenWay*, organizations can avoid the inevitable result of getting to the assessment process of the RMF and finding themselves run afoul of legal liabilities by missing requirements, controls or documentation. Additionally, when a scan, assessment or monitoring by the US CERT happens, the RMF approach leaves the organization open to not meeting their evidentiary and contractual responsibilities. *EigenWay* lays the ground work for the personnel, culture, process, documentation and A&A that not only redefines how to execute real Cybersecurity, it meets the intent of the USG.

Visit www.eigenspace.us to learn more about this new approach.

For Additional Information Contact:

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