The Future of Risk Management

I recently attended the Cloud Security Alliance Federal Summit in Washington DC. I felt the one day Summit was an just "ok". I was underwhelmed with anything new but overwhelmed by the continual push of almost ALL the speakers on "risk-based decisions" and "risk profile" and "risk mitigation" and "risk management". That got me thinking, why are we so risk heavy in our thoughts about Cybersecurity? And is that approach working?

First, what is the "risk management" paradigm. In most private sector organizations, corporate leadership and/or the Board of Directors focus on "Enterprise Risk". They want to know everything that could impact the organizational goals. That usually translates to financial impact to achieving the organizational goals. That, in my opinion, is a by-product of the makeup of most boards. They are all businessmen or businesswomen and focused on startup and/or growth of companies. In Federal agencies, risk is usually a governance and/or leadership worry about mission impacts. That, in my opinion, is a by-product of agency focus on accomplishing the mission at all costs. What is Cybersecurity Risk Management and how does it relate to these definitions?

There are many risk management models, but the most discussed and used one in the Federal context is NIST's Risk Management Framework (RMF). The origins of NIST's Risk Management Framework come from Federal Law. The E-Government Act and, specifically, FISMA are examples of what drives "risk management" within the Federal Government. To implement these concepts, guidance from OMB and FIPS 200 requirements were born. The concept that an organization can select security based on its own risk profile begins from this org and this document. We will come back to that. Then in the current iteration of FISMA, NIST is charged with providing the "how" Federal agencies achieve this risk management. NIST has published many publications to "help" with risk management under the "Risk Management Framework" umbrella. Documents like: SP 800-30, SP 800-37 (now draft rev2), SP 800-39, SP 800-53, SP 800-53a, SP 800-160 vol1 and vol2, SP 800-161, SP 800-171, SP 800-171a, NIST IR 8062, NIST IR 8179, and Cybersecurity Framework. Each one of these documents all drive the concept that you should do the following:

- **Categorize your IT System per FIPS 199/200**
- **Select the security controls required**
- **Implement the security controls that were approved**
- **Assess effectiveness of security control implementation**
- **Authorize the IT system for production use**
- **Monitor IT system for any anomalies, maintenance and continual effectiveness of controls**

I do NOT have an issue with this process. However, I DO have a problem with the way all the documents were written has created an environment where arbitrary people in the SDLC make

decisions that wittingly, unwittingly, knowingly and unknowingly compromise security in the name of "risk-based decisions". This violates the entire concept of Cybersecurity Awareness and Resiliency (CAR).

The new NIST SP 800-37 (draft rev2) describes the control selection and tailoring allowed. The language is confusing and allows for organizational interpretation. This breeds an environment for abuse. Let's take a closer look. From NIST SP 800-37 rev2 DRAFT, Chapter 3, Control Selection, Task 2, Discussion:

> *Discussion: There are two approaches that can be used for the initial selection of controls: a baseline control selection approach, or an organization-generated control selection approach. The baseline control selection approach uses control baselines, which are pre-defined sets of controls representing broad-based, balanced, information security and privacy programs that serve as a starting point for the protection of information and information systems. Security control baselines are selected based on the system security categorization (see RMF Categorize step, Task 1) and the security requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards. Privacy controls are selected based on a privacy risk assessment and privacy requirements derived from laws, executive orders, regulations, directives, policies, standards, guidelines, and stakeholder protection needs. Organizations can choose to develop or employ a privacy control baseline to select an initial set of privacy controls. Control baselines are provided in NIST Special Publication 800-53. After the appropriate pre-defined control baseline is selected, organizations tailor the baseline in accordance with the tailoring guidance provided (see RMF Select step, Task 3). The organization-generated control selection approach differs from the baseline control selection approach because the organization does not start with a pre-defined set of controls. Rather, the organization develops a set of security requirements using a life cycle-based systems engineering process (e.g., ISO/IEC/IEEE 15288 and NIST Special Publication 800-160, Volume 1) as described in the RMF Prepare-System Level step, Task 8. The requirements engineering process generates a specific set of security requirements that can subsequently be used to guide and inform the selection of a set of controls to satisfy the requirements. Similarly, organizations can use the Cybersecurity Framework to develop framework profiles as a set of organization-specific security requirements—guiding and informing control selection from NIST Special Publication 800-53. Tailoring at the system level may be required after the organization-generated control selection (see RMF Select step, Task 3). In instances where organizations do not use a baseline approach for selecting an initial set of privacy controls, the organizations can select privacy controls as part of an organization-generated control selection approach. References: FIPS Publication 199; FIPS Publication 200; NIST Special Publication 800-30; NIST Interagency Report 8062; NIST Special Publication 800-53; NIST Special Publication 800-160, Volume 1 (System Requirements Definition, Architecture Definition, and Design Definition Processes); NIST Special Publication 800-161 (Respond and Chapter 3); NIST Interagency Report 8179; CNSS Instruction 1253; NIST Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).*

The Future of Risk Management

How is this implementable from an entry level Cybersecurity role? (we will ignore for the moment an entire discussion on the applicability of the Cybersecurity Workforce Framework requirements for a Cybersecurity role). What controls achieve this mosaic of requirements, guidance, regulations and laws? This spans from architecture decisions to engineering tasks, from privacy to assurance, from Federal laws to agency policies, from vendor choices to supply chain issues. Note, none of what I just said is risk. It is just understanding what is in front of us to manage!!!!

Yet, I hear time and time again at conferences and throughout programs in the Federal Government that security was based on risk. Who makes the risk decision? Architecture? Engineering? Operations? Security? Mission? Executive Leadership? What are the risk decisions based on? Speed? Perceived Cyber risk? Mission risk? Financial risk? What vendors/products are being used based on these decisions creating Supply Chain Risk? What resiliency concepts are being used? What privacy issues are being addressed appropriately? What laws and regulatory compliance concerns are being addressed when these risk-based decisions are being made?

It is my opinion, that this complexity, coupled with rapidly changing technology, pressured by our insatiable appetite for instant gratification in the consumer world has driven us to just make quick uninformed decisions under the guise of risk management that wittingly unwittingly, knowingly, or unknowingly compromises Cybersecurity posture. This is why we are getting hacked on an exponential scale today…..

So, what would I do to change this?

My company, Eigenspace, was founded to do just that. We have scientifically changed HOW we approach the selection and tailoring of controls to avoid the abused risk-based decision mantra based on human bias. We honor the CAR and attempt to be Cyber Aware and Cyber Resilient in every decision we make. We leverage the Cybersecurity Order of Operations Methodology (COoOM) to create a "litmus test" to ensure we haven't missed any "angle" of thought during our security control selection process. This is a scientific way to create the selected security controls versus human biased "best practices" and "risk-based" decisions. To be clear, we ascertain all the required laws, regulations, and guidance, scientifically run down all the required controls for each, deconflict them, ensure all related controls are accounted for, ensure all derived controls are accounted for, ensure that the entire security control baseline that is established blends all the security controls together and score it for reference. This is the beginning point for security controls and, the EigenWay states that this is inviolate (meaning risk-based decisions can NOT de-select without evidentiary based justification that you are NOT violating laws or regulations or

The Future of Risk Management

introducing new risk by its de-selection). Then we believe that tailoring is the process of adding enhancements, supplementary controls or additional mitigations based on identified specific risks. Again, tailoring is not the minimization or removal of controls based on risk decisions. This is how Risk Management Framework has been abused and minimizes its effectiveness.

So, in summary, I believe NIST's RMF is being abused and is causing confusion and relaxed Cybersecurity postures in the Federal government protected by the "risk-based decisions" made under the RMF. If task 2 and 3 of RMF, selection of controls and tailoring of controls, respectively, were to follow the EigenWay, RMF could achieve its vision of organizing risk and ensuring Federal agencies correctly plan to protect information systems according to this risk.

For Additional Information Contact:

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