Are Cybersecurity Baselines Dead?

Compared to the "Iron Age", "Enlightenment", "Industrial Age", etc., today's "Information Age" is not that old, and, Cybersecurity younger still. We are constantly learning (sometimes the hard way) and we are maturing (or, in some cases, not) in this Cybersecurity industry to keep up with modern technological advances. Because we are so young as an industry, and I daresay immature as an industry, we should not only reflect where we have come but be secure in ourselves to say we have made mistakes along the way. But, most importantly, are we learning from them?

So, how did we get here? Of course, very early computers were VERY large machines. So physical security was paramount. Then program corruption and integrity became the next concern. The industry evolved through access control and many other security related challenges as it was developing. As one practitioner discovers or thinks of another attack vector, he/she documented and/or lets their peers know – and best practice and information sharing principles were born. But, intellectually, this best practice model isn't a comprehensive review of security, only a human biased focus (what we know). But it was new. It was better than before. It was easy to understand. It was easy to implement (a checklist). Thus, began an inadvertent new phenomenon: best practices become security.

As more and more best practices became known, system administrators and practitioners began listing them out. Once stakeholders, supervisors, and regulatory auditors wanted to ensure that all best practices were being followed, compliance checklists were borne. In today's Cybersecurity world, we are inundated with security Baselines, for example, FedRAMP, CIS Critical 20, DOD STIGs, USGCB, etc. In order to keep up with the evolution of technology, baselines are quickly changing to keep up as well. What we have inadvertently created is a culture of checklist mentality that changes with technology, solution and regulator's focus. I believe that truly understanding the WHAT, WHY and HOW a security control is implemented is completely lost when all our focus is "are we minimally compliant?"

We spend an enormous amount of resources in Cybersecurity trying to be compliant with baselines and standards. Is it working? How many of you have either said or heard someone say, "We are compliant, but we aren't secure?"

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 me that baselines are nothing more than an approved selection of security controls by a particular 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 of these important attributes (legacy and new, like confidentiality, assurance, integrity, privacy, operational, technological, managerial, organizational, etc.) is the name of the game going forward in Cybersecurity. The NIST SP 800-53rev5 creates states of each control that

must independently and cross-checked for is different states' applicability before final adjudication of accreditation. Dome 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 SSP would be **start with ALL 912 controls**. You would have to justify in your assessment evidence the de-selection of the control.

Given the monumental focus on understand each and every security control and its entire state and applicability, AND justify each control's de-selection for every SSP, then are baselines a dead construct?

For Additional Information Contact:

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