The ASA Model as Foundation for Estimating Cyber Security Tendency Profiles

TAG Cyber – navitend

For Public Release (Version 1.0) – August 22, 2017

Introduction

Through the experiences of cyber security and information technology industry veterans Edward Amoroso (TAG Cyber), Steven Spagnuolo (ZRG Partners), and Frank Ableson (navitend), combined with research and experimentation, the ASA Model has been developed to help describe an individual's personal tendencies in cyber security. The ASA Model focuses on tendencies in *technology, management,* and *compliance*, producing a three-factor output that fits into one of twenty-seven different personal profile vectors.

To make the ASA Model practically accessible, the *CyberEXP* tool was developed for use by cyber security professionals interested in greater self-awareness during career planning. The tool supports private self-evaluation using a questionnaire that was built on the ASA Model. Once the questionnaire is completed, the tool produces a report, including a breakdown of the measured tendencies, a description of the individual's profile, and a suggested learning plan.

This paper describes the basis for the ASA Model, including why the three dimensions of *technology, management, and compliance* make sense for cyber security professionals to evaluate. In addition, the process for creating the *CyberEXP* tool is explained and shown to accurately reflect an individual's tendencies for cyber security. These tendencies provide a basis for an individual to self-examine personal strengths and weaknesses with respect to desired career objectives.

Basis for ASA Model

The ASA Model encapsulates the three most important and defining personal tendencies[1] for success in cyber security.[2] Each of these personal tendencies—*technology, management,* and *compliance*—is measured independently of the others, as this model does not include mutual exclusion, although predictable exclusion often appears in the results. There are twenty-seven different combinations of the three tendencies. The goal is to create a customized profile vector for an individual, showing high, moderate, or low tendencies in the three areas.

It is important to note that measured tendencies are different than experiences or expertise; for example, a great lawyer could have tendencies that are more on the artistic side, or a construction worker could have tendencies toward technology. It is the same for cyber security. That is, anyone using the CyberEXP tool should not conclude that years of experience as a software developer immediately

[1] Def: Tendency: An inclination toward a particular characteristic or type of behavior.

[2] The likelihood that the ASA Model applies equally to general technology careers is high.

translate to high technology tendencies. In many cases, it might be just the opposite. For example, many great technical contributors have had to overcome a personal tendency that might lean toward hoping or expecting that some outside expert would figure out the details of some mechanism.

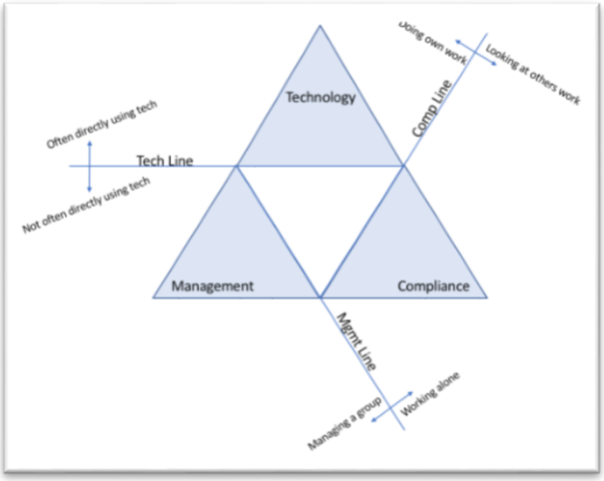

Figure 1: The ASA 3-Factor Model

The three factors in the ASA Model answer the following three basic questions: Do you possess personal tendencies that are consistent with work activity in technology? Do you possess personal tendencies that are consistent with successful work supervision? Do you possess personal tendencies that are consistent with the work of reviewers, auditors, and compliance assessors? These high-level questions can be answered with a yes or no, but the ASA Model recognizes that answers are more spectrum-based. By calculating scores for each tendency area, the ASA Model positions an individual on the spectrum represented in Figure 1 that corresponds with the given self-assessment values.

The model can be illustrated via three archetypes. The first is the gifted technologist who works best in isolation. This archetype is contained in the top corner of Figure 1 with high tendencies toward technology but low tendencies for management and compliance. Obviously, if this individual has self-expressed a goal of becoming a senior executive, then some learning and adjustments will likely have to be made.

The second archetype is the detail-oriented auditor who works alone and does not gravitate toward advanced technology. This archetype is contained in the bottom right corner of Figure 1 with high tendencies for compliance but low tendencies for technology and management. If this individual seeks to do more hands-on security tech, then learning and adjustments will likely have to be made.

The third archetype is the personable leader who manages teams, but does not work in isolation developing advanced security technology. This archetype is contained in the bottom left corner of Figure 1 with high tendencies for management but low tendencies for technology and compliance. Career plans for this type of compliance-oriented individual would have to be managed or adjusted according to the associated tendencies.

No archetype is better than any other, and a collage of different individuals with different tendencies are required to run a successful cyber security company. In addition, just because someone has weak tendencies in an area, does not preclude that individual from becoming successful in that area. One might even argue that having tendencies in areas that are separate from one's primary focus will result in strength through greater balance and diversity.

Technology Tendency

This tendency involves propensity to use tools, think conceptually, and apply metrics to solve problems, especially ones related to computer science and cyber security. The importance of technology in the cyber security industry is obvious. The creation, deployment, and upkeep of protection tools and services requires a high level of technical know-how. Without expert technologists, cyber security would be stripped of its main sophistication and progress-driving force. This tendency is associated with the following general rubric:

- You fearlessly dive into a complex challenge, fully confident that you will find a way to figure things out on your own.
- You are not satisfied knowing just what something does, but rather, you demand to understand at a meaningful level how it works and why.
- You are ready and willing to work with others, but deep down, you suspect that you would probably accomplish most tasks much better on your own.

While most computer scientists and cyber security professionals exhibit a higher understanding of technology than the average person, the ASA Model measures technology tendencies laterally inside the industry, where the benchmark 'low' tendency is already much higher than that of the average person. On the opposite side, a 'high' technology tendency suggests an impressively strong inclination for working with advanced technology.

Management Tendency

This tendency measures the propensity to effectively delegate, lead, and work with a group with *high integrity*. No cyber security team is equipped to deal with the disaster-prone nature of the industry without effective leaders. The skills required to stay organized and see the bigger picture in a time of crisis are what separates a mere grouping of talented technologists from a world-class cyber team. This tendency is associated with the following general rubric:

- You feel the need to coordinate groups of people toward honest, responsible, high-integrity approaches based on sound judgment.
- You are perfectly satisfied understanding how something works and how it can help others, leaving the underlying details to the experts.
- You are ready and willing to do tasks on your own, but deep down, you know that others are probably better suited to produce better results.

This tendency covers a wide area, but the ASA Model stresses the importance of honesty, good judgment, and integrity. For cyber security specifically, a good manager must handle crisis situations, work with gifted technologists, and lead detail-oriented compliance auditors. These tasks can be difficult due to the quirks and idiosyncrasies that emerge in cyber security staff personalities. The ability to manage such personalities is an important challenge in cyber security. The ASA Model is built on the presumption that tendencies toward honest judgment are the best predictors for good management skills.

Compliance Tendency

This tendency involves the propensity to rigorously audit and review the work of others. The cyber security industry is constantly in the shadow of looming attacks, bugs, and disasters. When such events inevitably occur, the most common response is for supervisors to suggest ramping up governance and compliance programs. While this approach may not necessarily be effective at increasing security, compliance programs are the most easily implemented improvements and defenses. This tendency is associated with the following general rubric:

- You feel compelled to organize chaos and complexity into meaningful structure so that it can be improved and understood.
- You are not satisfied with what something does, or even how it works, but rather, you seek to understand the nature of the process by which it was created.
- You have a deep sense of justice, and believe that shortcuts leading to poor quality must be prevented, perhaps even harshly.

Compliance auditors must be rigorous, detail oriented, and more than anything, thorough. Falling short of a requirement due to ignorance or oversight is an avoidable mistake and one that strong compliance employees will not make. The ASA Model measures compliance tendencies in terms of how likely a subject is to complete a task in an organized way that ensures complete and total confidence in the correctness of that task.

CyberEXP Tool

The challenge in determining an individual's tendencies is to remove the inherent bias associated with uncovering his or her personality traits. The first requirement in such establishment is to factor out any fears or agendas that might arise if someone's supervisor is expected to review the results of these tendency assessments. For this reason, we believe that the ASA Model can only be applied through private, honest, self-assessment. Enterprise security team managers and CISOs should consider the model a private tool for self-use by their team members, rather than something to be used for performance evaluation or promotional consideration.

In addition, the ASA Model is built on the assumption that people can trick or game a questionnaire, even if they intend to keep the results private. Everyone likes good news, so answering a questionnaire in a way that reinforces already-held beliefs is a challenge to overcome. Because of this, the CyberEXP tool implements the ASA Model through carefully-designed questions.

Three principles guided the development of the questionnaire. First, the best questions should engage the subject in a personal situation where a decision must be made. It is better to place the subject in a meeting where something is happening and the subject must respond rather than to introduce some abstract question about a theoretical response to a theoretic situation.

Second, the sequence of questions—just like life—jumps around a bit. Rather than have someone settle into a comfortable pattern, addressing similar issues in a section of the questionnaire, the CyberEXP tool instead presents scenario questions in a random manner so that the subject has less inclination to just pick an answer that follows from the previous one.

Third, the CyberEXP tool uses indirection to determine tendencies. For example, a direct approach would ask a subject: “Do you love technology more than pop culture?” to which anyone in cyber would roll his or her eyes and list technology as his or her preference. An indirect approach to establish tendency would instead do something like this: “You are about to answer a question for a million dollars: Be honest—would you rather it be a question about technology or pop culture?”

CyberEXP Learning Plans

Once an individual completes the personality assessment and receives a tendency profile, two unfavorable responses may occur. First, the assessment might be viewed as an entertaining curiosity (“Huh, so I guess I have moderate tendencies in all three areas. Oh, well.”) This is clearly not the goal in the establishment of the ASA Model, but it certainly does no harm if subjects do not take the results seriously. Second, the assessment might be misinterpreted as somehow incorrect or unfair, perhaps missing the obvious contributions and achievements of the subject in cyber security (“What! I am not moderate in all three areas! This is crazy!”) This is also not the goal of the ASA Model or CyberEXP tool, although this will clearly occur in a subset of subjects.

The desired outcome of the ASA Model report from the CyberEXP assessment is to produce thoughtfulness with respect to career planning. If a subject is a nerdy technician who hates managers and avoids compliance managers, then a result of Technology (High), Management (Low), and Compliance (Low) would reinforce currently held views. But what if the results are inverted? Suppose that nerdy tech obtains high tendency scores in Management. Perhaps this might spur some introspective consideration that new career opportunities might be on the horizon.

The CyberEXP tool includes learning plan recommendations as starting points for subjects who receive scores that are in some way surprising. The learning plans are also conditional in the sense that they try to determine the subject’s interests and plans. If a subject really wants to be a manger, but has a lower tendency score in that area, then some management training and assignments will be required in a learning plan. Similarly, if someone has never done compliance work, but receives high tendency scores in that area, then perhaps an “open assignment in the audit group” might be worth considering.

Concluding Remarks

It is surprising that cyber security teams invest so much time and effort into their technology, tools, systems, processes, and architecture, but invest comparatively little time in themselves. Certainly, managers try to mentor and offer career guidance, but the observer effect applies: by engaging in career planning, the manager affects and influences that planning. Private self-assessment, as found in the ASA Model and CyberEXP tool, is a superior approach.

In addition, while many learning plans presume that if you are an expert in an area, you clearly should drive your future activities in that area, an assessment based on *tendencies* will help identify paths of least resistance. If you are clearly not well-suited for management, but you are on that career track, then the CyberEXP results will help you at least recognize the rocky path you’ve chosen. Hopefully, most subjects using the tool will see the opposite results, confirming that they’ve chosen paths that perfectly match their tendencies.