Threat, Vulnerability Assessment [TVA]

Why TVA and not TVM? This is a good question and what I was thinking in 2005 was that I wanted to have a process in place where the IT, operational risk, second level and cyber employees could come to consensus on cyber risk using the result to make decisions on resource allocation. I thought, at the time, that this was more about a joint assessment (emphasis on the A for assessment). I've learned since that it wasn't necessary to emphasize "assessment" since TVA operates more like a risk management process. So TVM (threat, vulnerability management) is probably more accurate despite my initial misgivings many years ago. The question is, what is TVA or TVM and what is the purpose of this process?

I've learned that the easiest way to define TVA is to describe how it works. TVA unfolds as a daily ritual that enables the cyber operations team to collate data from diverse sources within a 24-hour span and contrast it with previous day's TVA results. Any significant deviations flagged during this process warrant discussion in TVA sessions. These sessions, typically excluding weekends and holidays but activated promptly in the event of cybersecurity incidents, are steered by a designated TVA analyst on weekdays. Prior to each session, the analyst gathers inputs from cyber operations and IT hygiene teams, reviews threat intelligence sources and scrutinizes deviations from the preceding 24 hours and their sources. Subject Matter Experts (SMEs), categorized by expertise, contribute insights during these sessions, rating deviations in patterns on a scale of 0-5. The risk score aids in gauging the urgency of response and informs decision-making on remediation priorities.

Participation in TVA sessions is open-enterprise-wide, contingent on attendance at an educational session describing the process. Even the CEO and executive leaders are mandated to undergo this training, fostering a shared understanding of cyber risk across the organization. Moreover, internal auditors are invited to attend TVA sessions with special invites going to external auditors. Anyone who has interest is encouraged to participate and learn.

In large enterprises, achieving consensus on resource allocation based on risk priorities can be arduous. For example, should we patch a specific server first and then do an application cutover or do the cutover and then patch? TVA streamlines this process, generating a daily cyber risk score for comparative analysis. The resulting TVA report encapsulates a spectrum of events, each assessed with a risk score. These scores, aggregated and weighted based on predetermined categories' significance, culminate in the daily TVA score. The formula's evolution over time, fine-tuned by data science resources, ensures alignment with organizational expectations. Furthermore, the TVA score's longitudinal analysis offers valuable insights into the evolution of cyber risk and control maturity within the enterprise. Increasing scores signify a burgeoning attack surface, prompting resource reallocation or control enhancement. Conversely, declining

scores indicate the maturation of cyber risk management programs and improved control efficacy.

Ultimately, the TVA-to-TVM transition signifies a shift towards proactive cyber risk management, fostering organizational resilience amidst evolving threats.

Any deviations that were substantial were candidates for discussion during the TVA session. We chose not to have TVA sessions on weekends and holidays, and we also decided to initiate a TVA session whenever there was a cybersecurity incident on a 24 x 7 basis. On any given weekday, the TVA session would be facilitated by a TVA analyst. The TVA analyst would prepare for the session by soliciting information from the cyber operations team and the IT Hygiene team (asset inventory, configuration management, vulnerability management) for workstations and servers (before cloud). The information sought was what was different from the previous 24 hours and what is the source of the information. The TVA analyst maintained a list of Subject Matter Experts (SMEs) who had access to source information by category. The TVA analyst would seek information that deviated from the previous 24 hours and then schedule the SME to present this information during the TVA session.

The TVA analyst decided on the priority for each of the events (deviation from the previous 24 hours) and call on the SME to share information for the benefit of everyone participating in that specific TVA session. The SME usually offered their perspective on what the deviation represented using a numerical value between 0 and 5.0. 5.0 was the highest risk score and 0 was the lowest score (it was extremely rare to have a 5.0 or a 0.0) for any event. Those participating in the session would debate the score and then come to consensus on an appropriate score facilitated by the TVA analyst. The score helped provide context for changes to decisions on remediation priorities if that was necessary. The higher the risk score, the more likely an immediate response was required which impacted other work effort for both cyber and IT professionals.

Anyone in the enterprise could participate in the TVA sessions if they agreed to sit through a TVA education session prior to the daily scheduled session which explained how the process worked. The CEO and the Executive Team were required to take the training and participate in at least one session. Once they did this, they could attend any TVA session in the future. Internal Auditors were allowed to attend TVA sessions any time they wished. Regulators and external auditors were invited to attend specific sessions.

In large and medium size enterprises it is sometimes challenging to get different parts of the organization to deal with facts and make difficult trade-off decisions on the allocation of resources based on priorities. TVA serves as a process to facilitate consensus on cyber risk. The output is a cyber risk score that can be compared to yesterday's risk score or last week's risk score or last year's risk score. Here is an illustration of what the daily TVA report can look like:

	Category	Event	Source	comments	Risk Score
1	Workstations/endpoints	Patch # 2008-2	CMDB	The patch was rejected on lab devices	3.1
2	Windows & Linux servers	Patch automatically installed on 12,304 servers out of 12,401 total	Patch automation vendor, CMDB	DevOps team servers did not accept the patch due to a configuration issue	3.5
3	End user/email	Successful phishing attack	TVA incident	Outbound attempt blocked in sandbox, no credential compromise	3.1
4	Security intelligence	Article in Politico on sophisticated spyware targeting cell phones	Politico	Pegasus spyware leak showed how iPhones are vulnerable	2.2
5		Over 10,000 credentials published in dark web	Recorded Future	Matched the credentials to specific users (142) and forced reset of the password	2.3
6		Nation state sponsored attacks using credential stuffing	FS-ISAC Threat Intelligence Committee	Hundreds of member firms impacted by these attacks in the past 30 days	2.4
7	Software security	Multiple supply chain poisoning events from compromised developer credentials to repo accounts	News feeds	IAM standards for developer repo accounts and cloud accounts are not currently being applied consistently increasing the risk of a software supply chain poisoning attack	4.1
8	Authentication	Credential stuffing attacks thwarted	Brand protection software vendor	Over 10,000 attempted attacks in 1 day blocked by malware protection vendor	2.9
	TVA score today				**3.1**
	TVA score yesterday				2.8

There are typically 6-10 major categories of events predetermined by the TVA team. The TVA score is calculated by taking the aggregate risk score for each category and multiplying it by a weighting number (e.g.: 60% or 10%) based on how important that category is to the enterprise. The category weightings are typically reviewed and adjusted either quarterly or monthly. The changes in weightings are influenced by changes in the top cyber risks at the enterprise level. As an example, software supply chain poisoning attacks from compromised repo credentials may be on the rise in the industry and so the weighting from this category should be reviewed and increased as a result.

The TVA score total is a combination of the category weighting applied to specific events and summarizing into a single risk number (0.0-5.0). The formula to calculate this from the inputs is simplistically represented as follows:

Event score [3.0] + event score within category [3.2] /2 for the total number of events = 3.1 x the category weighting 75% = 2.33. The category score is calculated to be 2.33. This can be compared to a category score last month of 1.75 indicating a clear increase month to month. This may be an indication of the need for additional investment or focus on the controls within this category since the risk is increasing over time.

The total TVA score takes the weighted outputs from each category and adds them together to come up with the daily score. I always engaged with data science resources to create the algorithm to calculate the TVA score and it typically evolved in complexity over time. After a few years, we made tuning adjustments to the algorithm so the output matched expectations. The score is only relevant when compared with another point in time, yesterday, last week or last year. The value of the TVA process is in achieving consensus on risk priorities across the enterprise so that better decisions on resource allocation can be made. If IT and Cyber staff understand the cyber risks of specific events, then they are more likely to respond accordingly. TVA also helps second level functions participate in and understand cyber risks to avoid situations where recommendations for risk management may differ between cyber and second level reviews. TVA results are often shared with board members and executive leaders providing context into decisions on resource allocation.

New or enhanced cyber programs benefit from understanding the relationship between the TVA score and control maturity at enterprise scale. TVA scores should be lower over time as more mature cyber risk management programs are fully implemented and control maturity increases. The evolution of the TVA score over time provides senior executives and board members with a reference point. Significant increases in TVA scores is a clear indication of the potential need for allocating more resources or enhancing controls to yield more favorable results. A TVA score that trends upward over time is indicative of an increasing attack surface for the enterprise while a downward trend in TVA score may suggesting higher resilience. In hindsight, the initial emphasis on Threat, Vulnerability Assessment (TVA) over Threat, Vulnerability Management (TVM) stemmed from a desire for consensus-building among IT and cyber professionals regarding risk priorities. However, as the process matured, it became evident that TVA operated more as a risk management mechanism. Thus, perhaps TVM is the right acronym and may be more apt going forward.