Using Threat Vulnerability Asset (TVA) Methodology to Identify Cyber Threats and System Vulnerabilities: A Student Field Project Case Study

Roberto J. Mejias, Colorado State University-Pueblo Pueblo, Colorado, U.S.A.
Morgan A. Shepherd, University of Colorado-Colorado Springs, Colorado Springs, Colorado, U.S.A.
Michael Fronmueller, University of Wisconsin-River Falls, River Falls, Wisconsin
Richard A. Huff, Colorado State University-Pueblo Pueblo, Colorado, U.S.A.

ABSTRACT
Research demonstrates that the use of vulnerability assessment (VA) tools are critical in identifying cyber threats and system vulnerabilities. This paper presents a case study of a student field project that utilized the Threat Vulnerability Asset (TVA) matrix methodology, an open source and uncomplicated VA tool to identify cyber threats and system vulnerabilities for a software engineering organization in the U.S. Southwest. The TVA methodology specifically helped the student project team identify and prioritize their client organization's most critical IT (information technology) resources, the cyber threats to those critical IT resources, the IT safeguards currently in place and identify the resulting system vulnerabilities from the triangulation of these three TVA matrix components. Additionally, the TVA methodology assisted the student project team to identify clear imbalances in the allocation of IT safeguards to certain critical and vulnerable IT resources. The implications for practitioners and educators from the results of this TVA field case study is that open source and uncomplicated VA tools such as the TVA methodology increase student pedagogy for the active learning of cyber threats and system vulnerabilities in our current IT-intensive environments.

Keywords: TVA methodology, cyber threats, threat vulnerability analysis, system vulnerabilities, vulnerability assessment methodologies, information security risk, student cyber security field projects.

INTRODUCTION AND BACKGROUND

As networks become increasingly complex via open architectures, multi-tiered networks, global web services and cloud computing storage, it has become increasingly difficult to protect critical organizational IT (information technology) resources and assets from new cyber attacks, data breaches, and system intrusions (Mejias and Balthazard, 2014; Sharmeli-Sendi et al., 2016). Approximately 90% of organizational information systems have been breached by unauthorized personnel (Ponemon Institute, 2018). Additionally, newer open information system (IS) architectures must increasingly allow external entities (i.e., vendors, contractors, suppliers) access to their internal networks, often inside of their organizational IS firewalls. In many cases these external entities require increased access to previously proprietary information that is critical to ongoing organizational operations and processes. Unfortunately, the demands of maintaining continued operations and profitability often take precedence over the protection of critical IT (information technology) resources and strategic data.

Multiple challenges continue to exist for organizations seeking to protect their IT resources and data from successful cyber attacks. The first challenge is identifying those IT resources and assets that are most critical to the core operations of their organization (Mattord and Whitman, 2018; Herath and Herath, 2014). Clearly, in order to remain competitive in a globally demanding environment, critical processes must continue to be productive and efficient without interruption (Ciampa, 2018). The second challenge is identifying those cyber threats most likely to affect or attack these critical IT resources and operations. If key IT resources, strategic data, and propriety information are not sufficiently protected, a successful cyber attack can quickly render an organization to be less competitive and non-operational for a significant period of time (Mejias and Balthazard, 2014). The third challenge is identifying the greatest vulnerabilities to these cyber threats by assessing whether current IT safeguards are adequately protecting these critical IT resources. Understandably, limited financial resources make it infeasible for IT management to protect all IT resources and processes while still maintaining profitability and continuity.

Protecting key IT resources may have an even greater effect for small-and-medium-sized enterprises (SMEs) (Osborn and Simpson, 2017), as is demonstrated in this current field case study. Shropshire, Warkentin and Sharma

Accepted for Publication, *Business Education Innovation Journal*, to be published in Vol. 11, No. 1, June 2019. Elm Street Press, LP

(2017) found significant variance among SME executives between adoption *intention* and actual *adoption* of information security measures. Adoption intention by non-IT personnel (i.e., upper management) in non-IT intensive industries was most influenced by IT budget limitations and the perceived severity of identified vulnerabilities (Osborn and Simpson, 2017). While executives were frequently found to be overconfident in the ability of their security systems to protect their key organizational resources, the use of periodic vulnerability assessment (VA) methodologies significantly increased their information security awareness (ISA) for potential cyber attack vulnerabilities (Bauer, Bernroider and Chudzikowski, 2017; Ponemon Institute, 2018; Shropshire, Warkentin and Sharma, (2017).

Research has demonstrated that the impact of cyber attacks may be reduced by the use of VA methodologies (Certified Ethical Hacker, 2017; Jenkins, Durcikova and Burns, 2013; Mejias and Balthazard, 2014). A *vulnerability assessment* has been defined as the systematic identification of an organization's most critical IT resources, the threats against those resources, the current safeguards in place to protect those IT resources, and the identification of the most vulnerable IT resources for that particular information system (Ciampa, 2018; Mejias and Balthazard, 2014; Certified Ethical Hacker, 2017). However, previous research has been vague and non-specific in describing the specifics and utilization of VA methodologies, particularly the Threat Vulnerability Asset (TVA) matrix methodology; a free, open source and readily available tool for identifying cyber threats and system vulnerabilities.

The paper presents a field case study of how a student project team, led by a faculty security expert, used the TVA methodology to generate a working TVA matrix that identified and prioritized critical assets and cyber threats, analyzed current IT safeguards, and identified system vulnerabilities from the triangulation of these three TVA components. The TVA matrix also provided useful insights for rebalancing the assignment of IT safeguards to better address the SME organization's greatest system vulnerabilities. We believe this field case study provides an uncomplicated but innovative approach to improve the current IT educational pedagogy for identifying cyber threats and system vulnerabilities.

REVIEW OF RESEARCH: VULNERABILITY ASSESSMENT METHODOLOGIES

Practitioners and researchers have examined numerous approaches to identifying cyber threat agents and system vulnerabilities. Effective VA methodologies, such as *OCTAVE* (Operationally Critical Threat, Asset, and Vulnerability Evaluation™), *VAMM* (Vulnerability Assessments & Mitigation Methodology), *CRAMM* (CCTA Risk Analysis and Management Method), and *TVA* (Threat-Vulnerability-Asset) have been utilized to facilitate the identification of critical IT resources, the threats to those IT resources, and the identification of related system vulnerabilities.

The OCTAVE® methodology as a VA tool provides a security framework for determining risk level and planning defenses against cyber attacks. OCTAVE® was originally developed as a VA methodology for U.S. military and logistics operations as a balanced approach to information security risk management. However, OCTAVE primarily focuses on organizational risk management and emphasizes strategic and tactical issues, with a lesser emphasis on the technological aspects of addressing information security risk (Alberts et al., 2003).

VAMM was created by the RAND Institute for the Defense Advanced Research Projects Agency (DARPA) and was developed to address the perceived weakness of other VA methodologies in identifying critical vulnerabilities and appropriate cyber security mitigation techniques (Anton, Anderson, Mesic and Scheiern, 2003). VAMM primarily focuses on software development and identifies a taxonomy of system attributes that generate system vulnerabilities. These identified vulnerabilities are then mapped to an appropriate list of IT safeguards that would most effectively mitigate those system vulnerabilities. VAMM was designed not only to mitigate and eliminate *identified* vulnerabilities, but to also identify previously *unknown* vulnerabilities in order to establish appropriate IT safeguards. However, like OCTAVE, the VAMM methodology is extensive, time consuming, and requires trained evaluators and specialized software tools to implement. The developers of VAMM acknowledge that after the initial three steps of the process "the methodology's complexity increases greatly" (Anton et al., 2003).

CRAMM was developed by the Central Computer and Telecommunications Agency (CCTA) of the United Kingdom government with the goal of providing a methodology to conduct information system security reviews (CCTA, 1988). CRAMM uses a structured automated analysis tool to identify and value assets, identify threats and vulnerabilities, calculate associated risk, and identify appropriate countermeasures. The CRAMM process requires

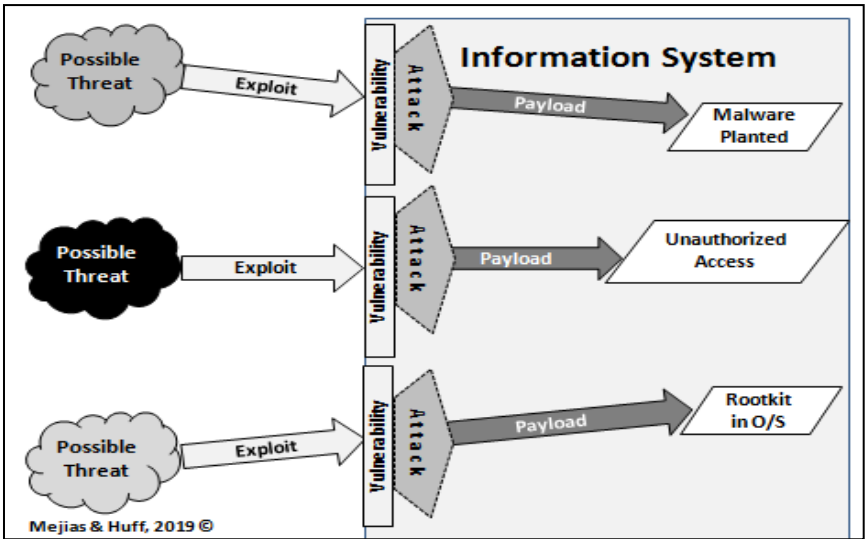
trained reviewers who gather data by interviewing organization personnel, which is then entered into the CRAMM analysis tool. The CRAMM process then assigns risk values to the various threats and vulnerabilities and recommends a hierarchical set of applicable countermeasures from a database of over 4,000 potential countermeasures. CRAMM reporting includes the cost of the recommended countermeasures and their relative impact. However, the CRAMM application constitutes a relatively expensive software investment and requires a significant amount of lead time to train reviewers for data input (Elof, Labuschagne and Badenhorst, 1993).

The TVA matrix methodology appeared to combine the best and most useful components of the OCTAVE, VAMM, and CRAMM methodologies and provided a free and relatively uncomplicated VA tool to systematically identify and prioritize IT assets, cyber threats, and system vulnerabilities. The TVA methodology was also selected for the current field project case study as TVA methodology has been increasingly used by cyber security educational programs that seek an open source and readily available VA methodology tool for training students and practitioners in identifying cyber threats and system vulnerabilities (Mejias and Balthazard, 2014; Renfroe and Smith, 2014).

The TVA project team in our field case study used the following components to develop and implement the TVA methodology matrix:

1. Identification of the organization's cyber security mission,
2. Identification and priority ranking of critical IT resources,
3. Identification and ranking of threats to IT critical resources,
4. Analysis of current IT safeguards and identified system vulnerabilities,
5. Recommendations of new IT safeguards (to address identified vulnerabilities).

Figure 1: Relationship between Cyber Threats, Exploits, Vulnerabilities, and Cyber Attacks



In implementing a viable TVA methodology, it was critical for the project team to understand the differences between *cyber threats*, *cyber exploits*, and *cyber attacks* (see Figure 1). *Cyber threats* are defined as any potential action that may compromise the confidentiality, integrity, and availability of an information system (Mejias and Balthazard, 2014; Ciampa, 2018), or that may violate information security policy (Bulgurcu et al., 2010; Chen et al., 2012; Flowerday and Tuyikeze, 2016). Cyber threats include, but are not limited to viruses, network worms, Trojan horses, denial of service (DoS) attacks, XML and SQL injection attacks, botnets, ARP attacks, and SCADA (supervisory control and data acquisition) attacks, or a multi-dimension combination of the above (Ciampa, 2018).

Cyber exploits refer to specific techniques or methods employed by cyber attackers seeking to breach a particular IS vulnerability or weakness (Simpson et al., 2010; Certified Ethical Hacker, 2017). Examples of exploits are reconnaissance, footprinting, scanning, packet sniffing, phishing, social engineering, wardriving, and hacking/cracking. A *cyber attack* is the successful materialization of a cyber threat via the deliberate exploitation of a particular IS security vulnerability (Ciampa, 2018).

A *vulnerability* is a flaw or weakness in the organization's IS design, implementation, security procedures, or internal controls (William and Mattord, 2018; Ciampa, 2018). System vulnerabilities are "exposures" that may succumb to various cyber threats and attacks that exploit system weaknesses and transform a *cyber threat* into a successful *cyber attack* (Mejias and Balthazard, 2014). As Figure 1 illustrates, a threat becomes a cyber attack when a particular exploit is successfully executed upon a system vulnerability (Mejias and Balthazard, 2014).

PHASES OF THE TVA METHODOLOGY

As previously discussed, the OCTAVE, VAMM, CRAMM, and TVA methodologies possess similar components that relate to the identification of critical assets, threats and system vulnerabilities. In the following sections we describe how our student project team used the TVA methodology as an uncomplicated VA tool to identify their client organization's critical assets, cyber threats and specific system vulnerabilities.

Identification of the Organization's Cyber Security Mission

Before any identification of critical IT assets and/or cyber threats were undertaken, the TVA project team first sought to identify their organization's cyber security mission. Security mission statements are often completely absent or not clearly established by management. This was the case with our current TVA field project. As the strategic and business goals of the SME's organization were better identified and articulated (often with assistance from TVA project team members), the organization's cyber security mission and related policies were more clearly formulated as the TVA project team continued their implementation of the TVA methodology. (The security mission statement related to the SME organization featured in this case study could not be disclosed in this manuscript due to non-disclose agreements).

Identification and Priority Ranking of Critical IT Resources

Identification of Critical IT Resources

Next, the TVA project team identified the core IT resources and processes that were critical to the ongoing operation and success of the organization. The systematic identification and prioritization of the organization's *most* critical IT resources allowed the TVA project team to focus on those critical IT resources that should receive the most protective attention (i.e., IT safeguards). Research, however, indicates that the identification of critical IT assets and resources is an evolving process and to date, there is still has no definitive or widely accepted standard (Ciampa, 2018). The following general categories however, provided an excellent "first pass" to identify, group, and rank critical the organization's critical IT resources (Ciampa, 2018):

- Personnel
- Processes, Operations
- Data and Information
- Software Applications (e.g., operating systems and security components)
- Hardware (e.g., system devices, network infrastructure components)

Priority Ranking of Critical IT Resources

While it is financially infeasible to safeguard all organizational resources, organizations must develop a prioritization criteria to identify those assets that generate the greatest impact to the success of their organization (Mejias and Balthazard, 2014; Mukhopadhyay, Chatterjee, Saha, Mahanti and Sadhukhan, 2013). Sawilla and Oh (2008) propose that organizations use an asset ranking algorithm where vertex weights are used as inputs to identify critical organizational assets. For example, a vertex may represent a critical IT asset, such as a web server or operations data center. A more *heavily weighted* vertex represents a more important or critical asset. Asset rankings using vertex weights help organizations determine the best allocation of their IT safeguards to protect their most critical IT assets and resources (Sawilla and Oh, 2008). Following this heuristic, our TVA project team used a *Critical Resource Prioritization* table (see Table 1) to identify and prioritize the organization's most critical IT resources according to the ranking criteria established by the organization's management. The four ranking criteria was determined by the organization's management team as shown below.

The "Criteria Ranking Weights" (e.g., 40%, 20%, 20%, and 20%) assigned to each criteria were determined by the managerial and financial functions of the organization's management according to their relative importance to their organization:

Criteria 1: Assets most critical to *market share*
Criteria 2: Assets with the most impact to *revenue*

Criteria 3: Assets that would be *most expensive to replace*
Criteria 4: Assets with the *most impact to client trust*

Table 1 illustrates the Critical Resource Prioritization table developed by the TVA project team and represents the first pass at identifying and ranking the target organization's IT resources from most critical to least critical (i.e., last column). The relative *impact* or contribution of each of the Critical Resource Assets for each of the four ranking criteria was also determined by organizational management. For example, the weighted asset value for the first two assets would be:

(0.7 x 40%) + (0.5 x 20%) + (0.9 x 20%) + (1.0 x 20%) = *76%* Weighted Asset Value
(0.8 x 40%) + (0.9 x 20%) + (0.7 x 20%) + (0.8 x 20%) = *80%* Weighted Asset Value

As shown in Table 1, the Critical Resource Prioritization Table indicated that the #1 critical resource for this organization was their *software program patents*, followed by *engineering intellectual property*, *operations and data base servers*, etc.

Table 1: Critical Resource Prioritization Table (Adapted from Whitman and Mattord, 2018)

Critical IT Resource/Asset	Criteria 1: Most Critical to Mktg.Share	Criteria 2: Most Impact to Revenue	Criteria 3: Most Expensive to Replace	Criteria 4: Most Impact to Client Trust	Weighted Asset Value (%)	Rank
Criteria Ranking Weight (1-100%)	**40%**	**20%**	**20%**	**20%**	**100%**	
		Relative	***Impact***			
Patented SW Operations Process	0.70	0.50	0.90	1.00	**76**	**4**
Engineering Intellectual Property (IP)	0.80	0.90	0.70	0.80	**80**	**2**
Software Program Patents	0.90	0.90	0.90	1.00	**92**	**1**
Supply Chain Mgmt (SCM) System	0.70	0.70	0.80	0.70	**72**	**6**
Skilled Labor Force	0.70	0.60	0.80	0.90	**74**	**5**
Operations and Data Base Servers	0.90	0.80	0.50	0.80	**78**	**3**
Company Website	0.60	0.60	0.50	0.60	**58**	**7**
Nationally recognized Scientists, Researchers	0.30	0.40	0.70	0.60	**46**	**8**
Legal Team	0.30	0.40	0.40	0.80	**44**	**9**

Identification and Ranking of Threats to Critical IT Resources

Identification of Threats

Organizations face a wide range of cyber and non-cyber threat agents, including natural disasters, sabotage, theft, human error, software and system failure, and technological obsolescence. While the TVA project team realized that the threat landscape for any organization would be constantly changing as evolving threats would continue in real time, the identification and ranking of current threat agents was the next step in identifying system vulnerabilities. The TVA project team worked closely with the organization's IT personnel to identify and rank the range of threats

that would most compromise the security, confidentiality, and availability of the organization's most critical IT resources.

Priority Ranking of Threats

If every threat agent or exploit was expected to be a successful cyber attack, any I.S. security initiative would quickly become too complex to sustain. The TVA project team therefore worked with the organization's IT staff to prioritize and rank the threat agents they had previously identified. Researchers and practitioners have frequently used *threat modeling* and *threat prioritizing* techniques for ranking potential threat agents. Threat modeling analyzes exploits used by cyber attackers, the motivation for the attack, and the types of attacks that may occur (Ciampa, 2018). Threat prioritization may use simple classifications (e.g., low, medium, high threat) or more complex ranking techniques such as a *Threat Prioritization Matrix* as illustrated in Table 2.

Table 2 illustrates the development of a Threat Prioritization Matrix and is based upon the estimated impact of various threat agents upon the organization's most critical IT resources. The *Estimated Impact of a Threat Agent* (column 2) used an assessment scale of 0 to 100 and was based upon information gathered from industry benchmarks of similar organizations as a potential threat agent.

Table 2: Threat Prioritization Matrix (Adapted from Whitman and Mattord, 2018)

1. Identified Threat Agents	2. Estimated Impact of Threat Agent	3. Likelihood of Attack	4. Probability of Loss if Threat Successful	5. Threat Prioritization Rating (Col 2 x 3 x 4)	6. Threat Ranking
Software Design Vulnerability Error	57	20%	65%	7.4	**7**
Theft of Intellectual Property (IP)	94	30%	95%	26.8	**1**
Physical Damage to PCs, Hard Drives	89	10%	40%	3.6	**10**
Human Error in Software or Mfg.	30	10%	15%	0.5	**12**
DoS Attack / Website Outage	74	20%	53%	7.8	**6**
Loss of Supply Chain Vendors	80	75%	40%	24.0	**3**
Open Ports on Routers, Firewalls	53	10%	44%	2.3	**11**
Password Cracking of IS	59	60%	53%	18.8	**4**
Sabotage to Operations, Process	74	40%	90%	26.6	**2**
Key Vendor and , Contractors Loss	66	15%	45%	4.5	**8**
Eavesdropping on Corp. Network, IS	66	15%	45%	4.5	**9**
Social Engineering of Employees	70	60%	40%	16.8	**5**

The *Likelihood of an Attack* (column 3) was the estimated probability that a particular threat agent would be successful upon this organization. The *Probability of Loss if Threat was Successful* (column 4) was the estimated probability (by IT personnel) that critical operations would be severely affected if that threat agent developed into a successful attack. The *Threat Prioritization Rating* (column 5) was the product of the first three columns (i.e., columns 2 x 3 x 4) and produced a threat prioritization rating. From the *Threat Ranking* (column 6), the TVA project team was able to identify the relative ranking of threats from most probable to least probable.

Analysis of Current IT Safeguards and Identified System Vulnerabilities

Once the TVA project team identified and ranked the organization's critical IT resources and the greatest threat agents to those IT resources, the TVA project team was able to identify and analyze the organization's *current* IT safeguards for their individual capacity to safeguard the effects of the identified cyber attacks to those critical IT resources.

Table 3 presents a *TVA Matrix Template* that illustrates the triangulation of the three components from the TVA methodology: ranked critical IT resources, ranked threat agents, and current IT safeguards. In the first row of the TVA matrix template, the TVA project team listed their organization's most critical IT resources, ranked from most critical to least critical as previously prioritized in Table 1 (Critical Resource Prioritization Table). It is important to note that the TVA project team included only *six of the nine* critical IT resources originally listed from Table 1. While the organization in this field case study identified a wider range of additional critical IT resources, the TVA project team compelled the organizational and IT management to focus on the protection of only their *most* critical organizational IT resources, emphasizing that it would be operationally and financially infeasible to protect *all* organizational IT resources. Subsequent studies and research may include a wider range of critical assets and most probable threat agents within a TVA methodology matrix environment.

Table 3: TVA Matrix Template

	Ranked Critical IT Resources *(Most Critical ===> Least Critical)*					
Ranked Threat Agents *(most to least probable)*	1. SW Program Patents	2.Engineering Intellectual Property (IP)	3.Operation and DB Servers	4.Patented SW Ops Process	5.Skilled Labor Force	6.Supply Chain Mgmt. System
1.Theft of Intellectual Property (IP)						
2. Sabotage to Programs, IP, Ops SCM						
3. Loss of SCM,Vendors						
4. Password Cracking of IS						
5. Social Engineering of Employees						
6. DoS Attack / Website Outage						
Current IT Safeguards *(Unranked)*	**S1** Firewalls; **S2** IDS/IPS; **S3** Anti-Virus SW; **S4** Double Authentication; **S5** Encryption; **S6** SETA, Policies					

The TVA project team used Column 1 of the TVA matrix in Table 3 to illustrate the ranking of threat agents from most probable to least probable. The Threat Prioritization Matrix previously illustrated in Table 2 shows the threat agents (from most to least ranked) listed as column 1 of TVA matrix template. The current IT safeguards employed by the organization were identified in the bottom row of the TVA matrix. These IT safeguards included both technical safeguards (e.g., firewalls, intrusion protection, etc.) and non-technical safeguards (e.g., SETA (security education training and awareness) and security policies) (Bauer et al. 2017; Mejias and Harvey, 2012). Once the project team identified these three key components of the TVA matrix, the triangulation of these components would reveal the potential system vulnerabilities within the client organization.

The Vulnerability Rating Worksheet in Table 4 illustrates how the TVA project team identified and ranked the system vulnerabilities for the SME organization. Column 1 lists the ranked critical IT resources identified from Table 1 (Resource Prioritization Table). The *Identified Vulnerabilities* (column 2) relate to the various threat agents identified from Table 2 (Threat Prioritization Matrix) that could affect the ranked critical IT resources (column 1). The *Weighted Asset Value* (column 3) is generated from the last column in Table 1. The TVA project team, together with the SME's IT staff, compiled the *Vulnerability Likelihood* (column 4) from the organization's IT audit logs, which detailed previous scanning and intrusion attempts of the organization's information system. The *Vulnerability Rating* (column 5) was the product of column 3 and column 4. Finally, the *Vulnerability Ranking* (column 6) prioritized the organization's *Ranked Critical IT Resources* from most (V-1) to least vulnerable (V-6).

Table 4: Vulnerability Rating Worksheet. (Adopted from Whitman and Mattord, 2018)

1. Ranked Critical IT Resource	2. Identified Vulnerabilities	3. Weighted Asset Value	4. Vulnerability Likelihood	5. Vulnerability Rating (Col 3 x Col 4)	6. Vulnerability Ranking
1.Software Program Patents	-Internal IP theft -External IP theft -Software failure -Social Engineering -SW design error	92	.25	23.0	V-1
2.Engineering Intellectual Property (IP)	-Internal theft -External theft -Social Engineering -Hacker Access	80	.20	16.0	V-3
3.Operations and Data Base Servers	-Brute force crack -Physical Damage -Hardware Failure -DoS Attack -SQL Injection -Power Failure	78	.15	11.7	V-5
4.Patented SW Operations Process	-Insider theft -Sabotage -SCM disruption	76	.25	19.0	V-2
5.Skilled Labor Force	-Competitor hire -Labor Strike -Social Engineering	74	.15	11.1	V-6
6.Supply Chain Mgmt (SCM) System	-Key Vendor Loss -Vendor IP Theft -Vendor failure	72	.20	14.4	V-4

The Vulnerability Rating Worksheet provided the TVA project team with a systematic approach to determine which critical organizational IT resources would require the most IT safeguards. However, the TVA project team noted that the *vulnerability rankings* in Table 4 were different from the *prioritized rankings* of the critical IT resources in Table 1. This finding was significant. It highlighted the perception that while certain critical IT resources had been prioritized higher than others, the calculated metrics of Vulnerability Rating Worksheet revealed that they were not as vulnerable to cyber threats as other critical IT resources. Based upon these previous matrices and iterations, the TVA project team generated the *Current State TVA Matrix* in Table 5. The organization's current IT safeguards are identified in the bottom row of the TVA matrix. Each intersection square of Table 5 specified the IT safeguard(s) that were assigned to each critical resource to address a particular threat agent.

For example, in Table 5 column 1 the #1 ranked critical resource ("SW Program Patents") indicates that the IT safeguards S1, S5, and S6 were assigned to address the "theft of intellectual property" threat. Likewise, the identified vulnerabilities for each cell of the TVA matrix indicated which critical IT resource utilized which IT safeguards and which critical IT resources were revealed to be completely unprotected (indicated by the large "Xs").

For example, Table 5 indicates that the #3 critical IT resource *Operations and DB Servers* reveals several unprotected vulnerabilities to sabotage, loss of SCM system vendors and social engineering, all of which did not appear be addressed by the current IT safeguards. Likewise, the #5 ranked threat agent, S*ocial Engineering of Employees*, generated several vulnerabilities across five critical IT resources that are not addressed at all by the organization's current IT safeguards.

Table 5. Current State: TVA Matrix

	Ranked Critical IT Resources *(Most Critical =====> Least Critical)* *"***V-*n*" = Vulnerability rating**					
Ranked Threat Agents*(most to least probable)*	***V-1*:** 1.SW Program Patents	***V-3*:** 2.Engineering Intellectual Property (IP)	***V-5:*** 3.Operation and DataBase Servers	***V-2:*** 4.Patented SW Ops Process	***V-6*:** 5.Skilled Labor Force	***V-4*:** 6.SCM System
1.Theft of Intellectual Property	S1, S5, S6	S1, S4,	S1, S2, S3, S5,	S1, S4, S5, S6	S6	S1, S2, S3, S4, S5, S6
2. Sabotage to Programs, IP, Ops, SCM	**X**	**X**	**X**	S1,S2,S3, S4,S5,S6	N/A	S1, S2, S3, S4, S5, S6
3. Loss of SCM Vendors	N/A	N/A	**X**	S4	N/A	S1, S2, S3, S4, S5, S6
4. Password Cracking	**X**	S1, S4	S1, S2, S3, S4,	S1, S2, S4, S5	S6	S1, S2, S3, S4, S5, S6
5. Social Engineering of Employees	**X**	**X**	**X**	**X**	**X**	S1, S2, S3, S4, S5, S6
6. DoS Attack / Website Outage	N/A	N/A	S1, S2, S3, S4, S5	S4, S5,	N/A	S1, S2, S3, S4, S5, S6
Current IT Safeguards *(Unranked)*	**S1** Firewalls; **S2** IDS/IPS (Intrusion Detection, Intrusion Protection System, **S3** Anti-Virus SW; **S4** Double Authentication; **S5** Encryption; **S6** SETA, Policies					

V-*n* = Vulnerability Rank; S*i* = Safeguard; *DoS* = Denial of Service Attack; *SCM* = Supply Chain Mgmt; *SETA* = Security Education Training and Awareness

Recommendation of New IT Safeguards

Using the TVA methodology, the project team was able to quickly identify and prioritize critical IT resources and threats agents, analyze current IT safeguards, and provide their organization's management with a logical overview of the organization's current system vulnerabilities. The Current State TVA matrix (Table 5) also revealed an *imbalance* in the distribution of IT safeguards for the protection of its ranked critical IT resources. Specifically, certain critical IT resources may have been assigned too many IT safeguards while other, more highly ranked critical IT resources, were not assigned enough safeguards. For example, the lowest ranked critical resource, supply chain management (SCM) vendors, was assigned a larger number of IT safeguards as compared to other more highly ranked critical and vulnerable critical IT resources (e.g., SW Program Patents and Engineering IP). This imbalance resulted in higher vulnerability to sabotage, password cracking, and social engineering threats to the organization's highest ranked and most vulnerable critical IT resources.

The analysis of the vulnerabilities revealed in Table 5 allowed the TVA project team to develop the *Proposed TVA Matrix* in Table 6. This analysis resulted in the identification of several new vulnerabilities. The TVA project team identified one new threat (ransom-ware and data encryption) and re-characterized a previous threat (T*hreat to Intellectual Property)*, to be included as *Internal and External Theft of Intellectual Property*(IP). Subsequent

iterations of the Proposed TVA matrix suggested recommendations for additional and more strategically placed IT safeguards to address these newly identified vulnerabilities.

From Table 6, the TVA project team considered a range of additional technical and non-technical IT safeguards (denoted in bold face in Table 6) including a vendor-supported honey pot (S8) and a redundant database (S9) to reduce the newly identified vulnerabilities to ransom ware and data encryption threat. Additional non-technical safeguards included *enhanced* SETA, information security policies (S6) and non-disclosure agreements (S7) as deterrence measures to dissuade potential hackers from attacking vulnerable IT targets (Bauer et al., 2017; Flowerday and Tuyikeze, 2016; Jenkins et al., 2013).

Table 6. Proposed TVA Matrix

	Ranked Critical IT Resources *(Most Critical =====> Least Critical)* *"***V-*n*" = Vulnerability rating**					
Ranked Threat Agents	***V-1*:** 1.SW Program Patents	***V-3*:** 2.Engineering Intellectual Property (IP)	***V-5:*** 3.Operation and DataBase Servers	***V-2:*** 4.Patented SW Ops Process	***V-6*:** 5.Skilled Labor Force	***V-4*:** 6.SCM System
1.External & Internal Theft of I.P.	S1, **S2, S4**, S5, S6	S1, **S2**, S4, **S5, S8, S9**	S1, S2, S3 S5, **S8, S9**	S1, S4, S5, S6, S9	S6	S4, S5, **S9**
2. Sabotage to Programs, IP, Ops, SCM	S1, S2, S4, S5, S6, S9	S1, S2, S4, S5, S6, S9	**S1, S2, S4, S5**	S1, S2, S3, S4, S5, S6	N/A	S4,S5, **S9**
3. Loss of SCM Vendors	N/A	N/A	**S2, S5, S7**	S4	N/A	S7, S9
4. Password Cracking of IS	**S1, S2, S4, S5, S6, S9**	S1, S4, S8 S9	S1, S2, S4, **S5, S9**	S1, S2, S4, S5	S6	**S5,** S9
5. Social Engineering of Employees	**S2, S4, S5, S6, S7, S9**	S2, S4, S5, S6, S7, S9	**S2, S4, S5**	S2, S4, S5	NA	S4, S6, S7,
6. DoS Attack / Website Outage	N/A	N/A	S2, S3, S4, S5, **S8, S9**	S4, S5, **S8, S9**	S2, S4, S5	S6, S8, S9
7.Ransom-ware & data encryption	**S2, S3, S4, S5, S8, S9**	**S2, S3, S4, S5, S8, S9**	**S2, S3, S4, S5, S8, S9**	**S2, S3, S4, S5, S8, S9**	**S6, S7, S9**	**S4, S5, S8, S9**
Proposed IT Safeguards *(Unranked)*	**S1** Firewalls; **S2** IDS/IPS (Intrusion Detection, Intrusion Protection System; **S3** Anti-Virus SW; **S4** Double Authentication; **S5** Encryption; **S6** Enhanced SETA, Policies; **S7** Non-Disclosure Agreements; **S8** Vendor HoneyPots; **S9** Redundant Database					

V-*n* = Vulnerability Rank; S*i* = Safeguard; *DoS* = Denial of Service Attack; *SCM* = Supply Chain Mgmt; *SETA* = Security Education Training and Awareness

The TVA project team also recommended that the particular IT safeguards (e.g., S1 Firewalls, S2 IDS/IPS, S3 Anti-Virus software, and S6 Enhanced SETA, Policies) could be maintained by the supply chain vendors instead of client organization. The Proposed TVA matrix in Table 6 represented an improved and more balanced allocation of IT safeguards that would more effectively mitigate the system vulnerabilities identified by the TVA matrix.

Identification of Cyber Threats and Vulnerabilities

The threat-vulnerability-asset matrix feature of the TVA methodology provided the SME organization and the TVA project team with a logical and systematic framework for identifying and prioritizing the organization's most probable threat agents and the organization's greatest system vulnerabilities. The TVA matrix also proved useful in identifying significant *imbalances* in the allocation of IT safeguards. As previously discussed, the Current State

TVA Matrix (Table 5) clearly revealed that the organization's highest *ranked* and most *vulnerable* critical IT resources had been assigned fewer IT safeguards than other less critically ranked IT resources.

This imbalance was *significant*. It revealed a critical misalignment in the protection of the organization's most vulnerable IT resources. The protection "imbalance" revealed by the TVA matrix also highlights a common misperception that while certain critical IT resources may be ranked higher than others, they may not be considered as vulnerable to cyber threats as other critical IT resources.

LEARNING IMPLICATIONS OF THE TVA METHODOLOGY

As malicious cyber attacks become more successful in breaching information systems and stealing intellectual property, organizations must become more judicious in protecting their critical IT resources (Mukhopadhyay et al., 2013; CyberEdge Group, 2016). The use of the TVA methodology as a free and uncomplicated VA tool for identifying cyber threats and system vulnerabilities has become increasingly appealing to both organizations and educators (Mejias and Balthazard, 2016). This implies that higher education courses in IT and cyber security have the opportunity to go beyond mere classroom lectures about cyber threats and how they may affect organizations. IT educators must provide an engaging pedagogy of applied projects and methodologies that interact with these important IT and cyber security concepts.

This field case study illustrates how the use of an uncomplicated vulnerability assessment tool (the TVA methodology) enables IT students to extend the pedagogy of simply identifying cyber threats and system vulnerabilities from classroom lectures into what Bloom's Taxonomy of Educational Objectives describes as learning that spans across several levels: *knowledge, comprehension, application, analysis, synthesis,* and *evaluation* (Bloom, 1956). A revision of this original taxonomy framework modifies and updates these learning levels to *remember, understand, apply, analyze, evaluate,* and *create* (Krathwohl, 2002). Both taxonomies attempt to help instructors understand the various levels of learning with the goal of enabling students to progress to the highest level: *create*. The use of the TVA methodology described throughout this paper guides the student project team and its members through all six levels of Bloom's revised taxonomy framework and in particularly the last three levels: *analysis* (of critical IT resources, cyber threats and IT safeguards), *evaluation* (of current IT safeguards to address system vulnerabilities revealed by the TVA matrix), and *creation* (by the students of a series of artifacts and deliverables resulting in a workable set of recommendations for the organization).

Most organizations view cyber attacks as unlikely and do not fully comprehend the impact of how a successful cyber attack may result in the loss of proprietary data, strategic information, and competitive market share (Ponemon Institute, 2018). Traditionally, the focus of cyber security software vendors has been on the detection and removal of malicious software and less on the identification of critical system vulnerabilities. The TVA methodology used in this field case study allowed the student project team and IT management to clearly identify logical cyber threats and vulnerabilities to its most critical assets and strategic IT resources.

Student project team members realized first-hand that total cyber security of all critical IT resources is a myth and that not all IT assets are of equal value. The project team also realized how the readily available and uncomplicated TVA methodology could be quickly and efficiently used in a *non-invasive* manner to quickly identify critical IT resources and the threat agents most likely to exploit them. The TVA methodology and related TVA matrix outlined in this paper was able to be quickly employed by a relatively unsophisticated group of student project team members with little professional training in cyber security or vulnerability analysis. This suggests that other computer-related courses, particularly with regard to pedagogical application of cyber security concepts, would also be able to use the TVA methodology as an effective tool to identify cyber threats and related system vulnerabilities.

LIMITATIONS

As expected, a single case study may not provide the sample size, statistical power, or predictive nature generated by a controlled lab research study. However, because of their particularly appealing design across several applied fields (e.g., IT, computer security), case studies have their particular strengths. Field case studies provide valuable insights and a better understanding of what may improve the field's knowledge base as supported by actual field practices (Tomorrow's Professor, 2016). Additionally, case studies provide a rich and holistic means of investigating what is often a complex phenomenon. That is, readers can learn vicariously from a case study, the particulars and nuances of

the researcher's narratives and descriptions (Stake, 2005). Because our field case study focused on a single illustration regarding the use of a particular VA tool (i.e., TVA methodology) to identify cyber threats and vulnerabilities, we cannot generalize the particular research findings from this field case study to the larger population. However with regard to case studies, Erickson (1986) contends that "...the general lies in the particular..." and what we learn from a particular case study can be transferred or prove useful to similar applications. Therefore, while we cannot generalize our findings to the larger population of VA research, we believe the findings of our TVA field case study illustrates interesting details of a single research instance and the context-dependent knowledge that may be valuable to both practitioners and researchers (Erickson, 1986).

Finally, while the TVA project team was guided by a faculty cyber security expert, it was comprised and undertaken by undergraduate students. And although the TVA project student team was able to identify a wide range of critical IT resources, threat agents, and vulnerabilities for their SME organization, the limited finances and time commitment of the SME organization compelled the TVA project team to limit the scope its TVA grid and its analysis. A more comprehensive VA evaluation, using licensed vulnerability and penetration test software, of known and unknown cyber threats and system vulnerabilities, would complement the current finding from this TVA case field study.

CONCLUSION

Research demonstrates that the use of vulnerability assessments (VA) tools are instrumental in identifying cyber threats and system vulnerabilities (Whitman and Mattord, 2018). This paper presents a field case study that focused on the description and development of an open source and uncomplicated VA tool, the TVA methodology, by a student project team analyzing a small-to-medium enterprise (SME) in the U.S. Southwest. The TVA methodology was selected as an open-source and effective VA tool that has been increasingly considered by cyber security educational programs that seek to increase the pedagogy for identifying cyber threats and system vulnerabilities. The TVA methodology was instrumental in helping the student project team identify and prioritize their client organization's most critical IT resources, the cyber threats to those critical IT resources, the IT safeguards currently in place to protect those IT resources and the resulting system vulnerabilities identified from the triangulation of these three TVA matrix components.

The TVA matrix also provided useful insights for the student project team by identifying clear imbalances in the allocation of IT safeguards to certain critical IT resources. Specifically, the use of the TVA matrix revealed that many of the organization's highest ranked and most vulnerable critical IT resources had been assigned the fewest IT safeguards against the organization's most probable threats. For this particular student field project, the TVA matrix revealed that the *social engineering* threat appeared to create the greatest unaddressed system vulnerability across a majority of their client organization's critical IT resources. As educators are increasingly compelled to provide applied projects and methodologies that interact with their classroom concepts to support what Krathwohl (2002) termed the "higher learning levels" of *remember*, *understand*, *apply*, *analyze*, *evaluate*, and *create* from his revised taxonomy of Bloom's Taxonomy of Educational Objectives (1956), we believe this field case study provides an innovative approach to improve the current IT educational pedagogy for identifying cyber threats and system vulnerabilities in our current IT-intensive environment.

References

Alberts, C.J., Behrens, S.G., Pethia, R.D., and Wilson, W.R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠) Framework, Version 1* (CMU/SEI-99-TR-017, ADA367718). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13476.

Alberts, C.J., Dorofee, A.J., Stevens, J.F., and Woody, C. (2003). *Introduction to the OCTAVE Approach*. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546.

Anton, P.S., Anderson, R.H., Mesic, R., and Scheiern, M. (2003). *The Vulnerability Assessment & Mitigation Methodology*. RAND National Defense Research Institute. Retrieved from http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1601.pdf.

Bauer, S., Bernroider, E.W.N., and Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, *Computers and Security*, 68, 145-159.

Bloom, B. S.; Engelhart, M. D.; Furst, E. J.; Hill, W. H.; Krathwohl, D. R. (1956). *Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain.* New York: David McKay Co.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information system awareness. *MIS Quarterly*, 34(3), 523-548.

Certified Ethical Hacker. Ethical Hacking and Countermeasures: Threats and Defense Mechanisms, Second Edition, Book 2 of 4 (2017). Cengage Learning, Boston, MA.

Chen, Y., Ramamurthy, K., and Wen, K.W. (2012). Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157–188.
Ciampa, M., (2018). Security+ Guide to Network Security Fundamentals, 6TH Edition, Course Technology, Cengage Learning, ISBN-13: 978-1-337-28878-1 and ISBN-10: 1-337-28878-0.
CyberEdge Group (2016). Cyber Threat Defense Report; https://www.fidelissecurity.com/resources/cyberedge-group-2016-cyberthreat-defense-report,
CCTA (1988), A Guide to CRAMM for Management, Information Technology Security UK CCTAJ 0079, London.
Elof, J.H.P, Labuschagne, L. and Badenhorst, K.P. (1993). A comparative framework for risk analysis methods, *Computers and Security*, 12, 597-603.
Erickson, F. (1986). Qualitative methods in research on teaching. In M.C. Whittrock (Ed.), Handbook of research on teaching. (3rd ed.) Tappan, NJ: Macmillan. 119-161.
Flowerday S.V. and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who; *Computers and Security*, 61: 169-183
Herath, H.S.B., and Herath, T C (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems*, *57*(1), 54–63.
Jenkins, J., Durcikova, A., and Burns, M.B. (2013). Simplicity is Bliss: Controlling Extraneous Cognitive Load in Online Security Training to Promote Secure Behavior. *Journal of Organizational and End User Computing*, 25(3), 52-66.
Krathwohl, D. (2002). A Revision of Bloom's Taxonomy: An Overview, *Journal of Theory Into Practice*, 41(4), 212-218.
Mejias, R.J., and Balthazard, P. (2014). A Model of Information Security Awareness for Assessing Information Security Risk, *Journal of Information Privacy and Security*, Winter, 10, 1-26.
Mejias, R.J., and Harvey, M. (2012). A case for information security awareness programs to protect global information, innovation and knowledge resources. *International Journal of Transitions and Innovation Systems*, *2*(3-4), 302-324.
Mukhopadhyay, A.,Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S.K. (2013). Cyber-risk decision models: to insure IT or not? *Decision Support Systems and Electronic Commerce*, 56, 11–26.
Osborn, E., and Simpson. (2017). On small-scale IT users' system architectures and cyber security: A UK case study, *Computers and Security*, 31(7):27-50.
Ponemon Institute (July 2018). Cost of Data Breach Study: Global Overview, Benchmark research sponsored by IBM Security
Renfroe, N.A., and Smith, J.L. (2014). Threat/Vulnerability Assessments and Risk Analysis, Applied Research Associates, Inc. Retrieved from http://www.wbdg.org/resources/riskanalysis.php.
Sawilla, R. E., and Ou, X. (2008). Identifying critical attack assets in dependency attack graphs, *Springer Berlin Heidelberg*, 18-34
Sharmeli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA), *Computers and Security*, 57:14-30.
Shepherd, M.M. and Mejias, R.J. (2016). The Effects of Non-Technical Deterrence on Reducing Employee Internet Abuse Frequency, *International Journal of Human Computer Interaction*, 32 (7), 557-567.
Shropshire, J, Warkentin M. and Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior *Computers & Security*, 49, 177-191.
Simpson, M.T., Backman, K., and Corely, J. (2010). Hands-on Ethical Hacking and Network Defense, Second edition. Boston, MA: Thompson Course Tech.
Stake, R.E. (2005). Qualitative case studies. In N.K. Denzin & Y.S. Lincoln (Eds.) The Sage handbook of qualitative research (3rd ed.) (pp. 443-466). Thousand Oaks, CA: Sage.
Tomorrow's Professor (2016). Stanford Center for Teaching and Learning http://cgi.stanford.edu/~dept-ctl/tomprof/posting.php?ID=1013.
Whitman, M.E. and Mattford, H.J. (2019). Management of Information Security, 6th Edition. Course Technology,Cengage Learning. ISBN-13: 978-1337405713 and ISBN-10: 133740571X.