Risk Assessment & Mitigation in Defensive Cyber-warfare

Version 1.1, April 4, 2016

John J. Szucs, Venio, Inc.

Kurtis L. Warner, Venio, Inc.

Michael M. Cho, Venio, Inc.

Jason W. Cronin, Venio, Inc.

Will Moore, Venio, Inc.

Thomas C. Paris, Venio, Inc.

Tiera Thompson, Venio, Inc.

1 Abstract

Discovering and mitigating technological vulnerabilities is important, but being able to estimate the associated risk to the organization is just as, if not more important.

By following the approach described in this document, it is possible to estimate the severity of accumulated risk to any given system, enclave, application or service. It also becomes possible to estimate the impact on the organizations mission if a loss does occur.

In this way we can then make informed decisions about what to do about those risks given a finite set of resources. Having an unbiased and objective system in place for rating risks will save time and help reduce time-consuming and distracting debates about priorities. This system, the Risk Management Knowledgebase (RMK), will help to ensure that the organization does not get distracted by minor risks while ignoring more serious risks that are less well understood.

Ideally there would be a universal risk rating system that would accurately estimate all risks for all organizations. However, a vulnerability that is critical to one organization may not be as critical to another. Therefore a basic framework is presented here that should be *customized* for any given organization.

The authors have endeavored to make this model simple to use, while keeping enough detail for accurate risk estimates to be made. Please refer to the section below on customization for more information about tailoring the model for use in a specific organization.

1.1 Risk Model

RMK is based on a two-factor risk index, widely used in standard risk management methodologies and frameworks such as the Joint Enterprise Risk Assessment Model (JERAM) (United States Cyber Command, 2014). The factors in the risk index are:

- The **exploitability** of the risk. In defensive cyber-warfare, this refers to the ease of successfully exploiting the particular vulnerability in a cyber-attack. For example, an attack that does not require authentication, can be exploited from a remote network connection (such as the Internet), and is simple to use is considered to be highly exploitable.
- The **impact** of the risk being realized. This is sometimes referred to as the *severity* of the risk. In defensive cyber-warfare, impact refers to the degree of harm that would be caused by a successful cyber-attack on a given target or set of targets using a particular vulnerability. The impact of a cyber-attack can include (but is not limited to) disclosure of confidential or classified information, disclosure of Personally Identifying Information (PII), Personal Health Information (PHI), financial or materiel loss, degradation or disruption of mission capabilities, physical injury, or loss of life.

In RMK, both the exploitability and impact factors are quantified on a scale with the range 0 through 10. The score of 0 represents the lowest level of exploitability or impact and 10 representing the highest level.

Factor values can be verbally categorized per Table 1below.

Exploitability and Impact Levels	
0 to <2	Very Low
2 to <4	Low
4 to <5	Medium
5 to <7	High
7 to 9	Very High

Table 1: Exploitability and Impact Levels

Together, the exploitability and impact values can be used to produce a composite risk index, as defined in Table 2.

Exploitability	Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Low (11)	Medium (16)	High (20)	Very High (23)	Very High (25)
High	Low (7)	Medium (13)	Medium (18)	High (21)	Very High (24)
Moderate	Low (4)	Low (8)	Medium (15)	Medium (19)	High (22)
Low	Very Low (2)	Low (5)	Low (9)	Medium (14)	Medium (17)
Very Low	Very Low (1)	Very Low (3)	Low (6)	Low (10)	Low (12)

Table 2: Composite Risk Index

1.2 RMK and CVSS

The RMK methodology for risk assessment and mitigation is integrated with and reuses some concepts from the Common Vulnerability Scoring System (CVSS). CVSS was developed as an open standard by the Forum for Incident Response and Security Teams (FIRST). CVSS 3.0 was released while the RMK methodology was in development and this (current) version of the RMK methodology is based on CVSS 2.2. A future revision of this work will address CVSS 3.0 while retaining backward-compatibility with CVSS 2.2.

2 Evaluating Individual Vulnerabilities

2.1 Impact

In RMK, the impact factor (denoted by the variable I) for a single vulnerability has two major components:

- I_{CVSS}: The Impact Sub-score, as defined by CVSS.
- *CyTS*: A Cyber-Terrain Score, which quantifies the importance of a device or other network node to the organization.

2.1.1 Impact Sub-score (I_{CVSS})

As noted above, the Impact Sub-score is defined by the CVSS standard. To summarize, this score represents the effect of an (potential or actual) attack on the Confidentiality, Integrity, and Availability of a device or other network node.

The Impact sub-score has the range 0…10, where 0 represents no impact and 10 represents the worst possible impact.

Note that the Impact sub-score intentionally ignores business/operational context, which is addressed by the Cyber-Terrain Score (see Section 2.1.2). A vulnerability that would completely compromise the Confidentiality, Integrity, and Availability of an application would have an Impact sub-score of 10, regardless of the business/operational value of the application to the enterprise.

2.1.2 Cyber-Terrain Score (*CyTS*)

To assess the risks associated with operating in an interconnected world, it is imperative that organizations understand the mission impact of the complete loss of, or degraded capability in, a given information technology system.

RMK's Cyber-Terrain Score (CyTS) quantifies this into a value in the range 1…10, with 1 representing the least importance and 10 representing the greatest importance to the organization. This is an absolute, not a relative, scale and multiple systems may have the same CyTS. Also, it is important to note that a CyTS may be adjusted over time based on the emergence of new missions, or the elevated importance of a current mission.

Table 3 provides general guidance as to where certain impact factors should be scored. (Defense Information Systems Agency, Cybersecurity Range Branch (RE22),

2015) provides a more comprehensive scoring rubric for the US Department of Defense and its subordinate organizations. This scoring rubric can also be used as a model for other organizations to develop their own scoring rubrics. Neither of these sets of guidelines are all inclusive, and should only be considered as guidelines for the person assigning a CyTS to an information system. Judgment and experience are also two essential factors that will guide the scoring individual as they assign appropriate CyTS values.

Description of Impact	Score
Loss of Life	10
Inability to execute or complete mission	9
Compromise of Personal Health or Privacy Data	8
OPSEC Violation	8
Inability to complete full mission	8
Federal Regulation or Law Non-Compliance (other than Privacy & HIPPA/HITECH)	7
Complete Loss of a System / Application / Infrastructure for greater than 14 days	7
Contractual Non-Compliance	6
Adversaries' capabilities increased	6
Effect on Future Capabilities	5
Loss or effect on associated systems	5
Public Affairs (Public Incident)	4
Mission Performance Degradation (Limited, Moderate, Severe)	5, 7, 9
Economic Impact (Organizational, DoD, National)	4, 6, 8
Loss of Logistical support	6-8
Degradation of C2	7-9
International impact	6-8

Table 3: Cyber-Terrain Scoring Guidelines

The rubric breaks down the elements to assess in order to more accurately assign a CyTS given an understanding of the factors and the relative importance of the system in completing the organization's mission. It is important to note that the CyTS is a measure of the overall relative importance of the mission supported by the system and not just the immediate value of the system to its direct end-users.

2.1.3 Composite Impact Score

The composite impact score for an individual vulnerability is calculated from the impact sub-score and the CyTS per Equation 1.

$$I = 0 \leq (CyTSk_1)[I_{CVSS}k_2 + 0.5] \leq 10.0$$

Equation 1: Composite Impact Score

where:

- I is the composite impact score, with a range of 0…10.
- I_{CVSS} is the CVSS impact sub-score.

- $CyTS$ is the cyber-terrain score, defined in Section 2.1.2 with a range of 1…10.
- k_1 is a constant that represents the relative weight of the CyTS in the composite impact score. The default value of this constant is 1.43 and may be tuned for specific applications.
- k_2 is a constant that represents the relative weight of the CVSS impact sub-score in the composite impact score. The default value of this constant is 0.0555 and may be tuned for specific applications.

2.2 Exploitability

For vulnerabilities with associated CVSS scores, such as those in the Common Vulnerabilities and Exposures (CVE) dictionary, the base value for the RMK exploitability sub-score is the CVSS exploitability score. For vulnerabilities defined by a Security Technical Implementation Guide (STIG), the base value for the RMK exploitability sub-score is mapped from the STIG category per Section 4.1.

2.2.1 Network Security Domains

The base exploitability score for an individual vulnerability may be modified by the top-level network security domain to which the network device is connected. Essentially, more restricted network security domains reduce the AccessVector term in the CVSS Exploitability calculation by one or more levels. This reflects the higher levels of layered security controls inherent in the classified network security domains.

The CVSS 2.2 Exploitability formula is as follows:

$$Exploitability = 20 * AccessComplexity * Authentication * AccessVector$$

Equation 2: CVSS Exploitability

Table 4 provides the CVSS-defined values of the AccessVector term for reference.

AccessVector	Value
Local (AV:L)	0.395
Adjacent Network (AV:A)	0.646
Network (AV:N)	1.0

Table 4: CVSS AccessVector Values

From the equation and Table 4, one can calculate a modifier to the base exploitability to account for the network security domain, per Table 5. This modifier is referred to by the variable name *DomainModifier*.

As an example, the *DomainModifier* for a device connected to the NIPRNet is $20 * (1.0 - 0.646) = 7.08$, where 20 is the constant from Equation 2, 1.0 is the AccessVector value for AV:N and 0.646 is the AccessVector value for AV:A (one step lower), from Table 4.

Network Security Domain	Classification Level	Exploitability Modifier
Internet	UNCLASSIFIED	0.0
NIPRNet	Sensitive But Unclassified (SBU)	-7.08
SIPRNet	SECRET	-12.1
JWICS NSAnet Other compartmented (SCI) or special category (SPECAT) networks	SECRET//SPECAT TOP SECRET TS//SCI	

Table 5: Exploitability Modifiers for Network Security Domains

2.2.2 Malware Protection Modifier

Compliance with anti-virus/malware protection policies can reduce the probability that an attacker may successfully exploit a vulnerability through, for example, a Trojan horse attack. This modifier is represented by Equation 3.

$$AV = 10 \times AVR_{weight}(0.0 \leq \frac{(AVR_{age} - AVR_{grace})}{AVR_{limit}} \leq 1.0) + AVS_{weight}(0.0 \leq \frac{(AVS_{age} - AVS_{grace})}{AVS_{limit}} \leq 1.0)$$

Equation 3: Malware Protection Modifier

In the equation:

- AV is the malware protection modifier.
- AVR_{weight} is the relative weight given to malware protection/anti-virus reporting. The recommended value for this is 0.125.
- AVR_{age} is the age (in days) of the most-recent malware protection/anti-virus scan report from the device in question.
- AVR_{grace} is the grace period (in days) for malware protection/anti-virus reporting. The recommended value for this is eight (8) (days).
- AVS_{weight} is the relative weight given to malware protection/anti-virus updates. The recommended value for this is 0.125.
- AVS_{age} is the time (in days) elapsed since the most-recent update to the malware protection/anti-virus software and database on the device in question.
- AVS_{grace} is the grace period (in days) for malware protection/anti-virus updates. The recommended value for this is eight (8) days.

Note that in CMRS, anti-virus reporting and updates each represent 25% of the total score, for a combined weight of 50% of the total score. In contrast, RMK's recommended values for AVR_{weight} and AVS_{weight} and its limits on modifiers (see Section 2.2.4) place significantly less weight on anti-virus/malware protection. This is consistent with current best practices in which anti-virus/malware protection is an important part of a comprehensive, defense-in-depth strategy (Magnotti, 2015) but cannot be solely relied upon to protect against new or advanced threats.

2.2.3 De-Militarized Zone (DMZ)

For devices on the US Department of Defense NIPRNET, the exploitability of a given vulnerability may be modified by the location of the device within the so-called De-Militarized Zone (DMZ) architecture.

NIPRNET DMZ Location	DMZ Modifier	Notes
Connected to a network other than NIPRNET	+0.0	
Unrestricted (public access)	+0.708	Negates Network Security Domain modifier (see Section 2.2.1)
Private (accessible only from other devices connected to NIPRNET)	+0.0	Already accounted for by Network Security Domain modifier (see Section 2.2.1)
Restricted (CAC authentication required)	-0.22	Equivalent to changing CVSS Authentication factor from Single (Au:S) to Multiple (Au:M)

Table 6: DMZ Modifiers

2.2.4 Composite Exploitability Sub-Score

The composite exploitability sub-score is essentially the sum of the base exploitability sub-score (defined by CVSS) and its modifiers. However, the modifiers cannot reduce the exploitability score by more than 33% of its base value and the composite score remains limited to the range 0…10, like the base exploitability sub-score. This is expressed in Equation 4.

$$Exploitability = Exploitability_{Base} + (-\frac{Exploitability_{Base}}{3}) \geq \sum_{m \in modifiers} modifiers_i \leq (\frac{Exploitability_{Base}}{3})$$

Equation 4: Composite Exploitability Sub-score

In the equation:

- *Exploitability* is the composite exploitability sub-score.
- $Exploitability_{Base}$ is the base exploitability sub-score (as defined by CVSS).
- *modifiers* is the set of all modifiers, as defined elsewhere in this section.

2.3 Estimating Probability of Compromise

In our initial work, we estimated the probability of compromise associated with a particular vulnerability using the simple approach proposed on page 75 of (Lippmann, Riordan, Yu, & Watson, 2012), shown in Equation 5.

$$P_{compromise} = \left(\frac{Exploitability}{10}\right)^2$$

Equation 5: Estimated Probability of Compromise after Lippman, et al.

In the equation:

- $P_{compromise}$ is the possibility of the system in question being compromised using the vulnerability in question.
- *Exploitability* is the composite exploitability score, as defined in Section 2.2.4.

However, after initial real-world tests, this approach was found to be unsatisfactory. The probability of compromise declined too rapidly as the exploitability sub-score declined. Also, due to floating-point precision limitations, when large groups of vulnerabilities and affected network devices and enclaves were aggregated, the aggregate probability of compromise could actually decrease as the number of individual elements increased.

We identified the following desired characteristics for an improved function to estimate probability of compromise from an exploitability sub-score:

- At *Exploitability*=10, $P_{compromise}$ must be 1.0 (100% estimated probability of compromise).
- At *Exploitability*=0, $P_{compromise}$ must be 0.0 (no possibility of compromise).
- The $P_{compromise}$ domain should have a relatively shallow curve at the top (0.8…1.0) and bottom (0.0…2.0) ends of the *Exploitability* range.
- In the mid-range of *Exploitability* (2.0…8.0), $P_{compromise}$ should have a sharp curve.

We then evaluated various candidate functions against this requirement, as shown in Figure 1.

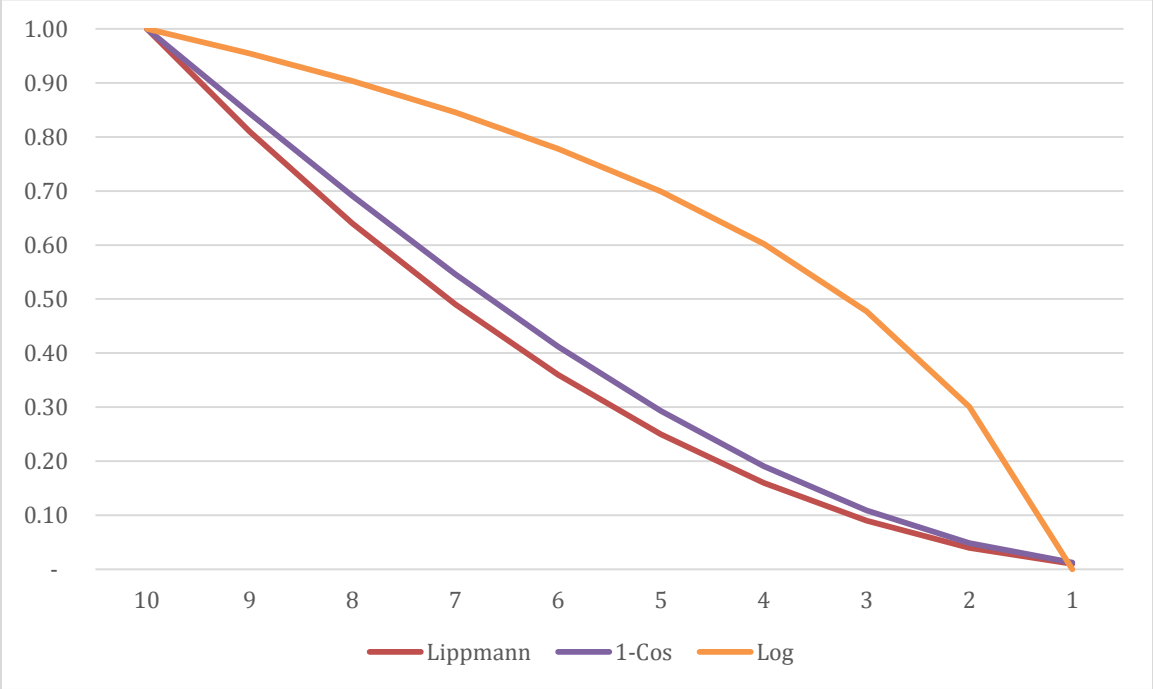

Figure 1: Candidate Functions for Estimating Probability of Compromise

In this chart, the "Lippman" series uses Equation 5, above. The "Log" series uses a simple logarithmic scaling function. The "1-cos" series uses a new function, presented in Equation 6.

$$P_{compromise} = 1 - \cos\left(\frac{\pi \times Exploitability}{20}\right)$$

Equation 6: Final Function for Estimating Probability of Compromise

In this function, the probability of compromise is estimated along a cosine curve, with the exploitability scaled from its original range of 0…10 to a working range of 0…1. As shown in Figure 1, this new function is similar to Lippmann but dampens less aggressively in the mid-range. Based on this comparison, we have selected this function for our work.

For our intended applications, it is also necessary to be able to convert from a probability of compromise to a CVSS-like exploitability sub-score. The two values are similar in concept, but not interchangeable. To perform the necessary conversion, we algebraically derived Equation 7 from Equation 6.

$$Exploitability = 10\left(\frac{2\cos^{-1}(1 - P_{compromise})}{\pi}\right)$$

Equation 7: Exploitability Sub-score as a Function of Probability of Compromise

3 Aggregating Vulnerabilities

A higher level of analysis is to quantify aggregations of known vulnerabilities across physical or logical groupings:

- A single network device
- A group of network devices in an enclave
- Multiple devices and enclaves in an organization.
- Subordinate elements of an organization.
- Other logical or physical groupings.

3.1 Aggregate Probability

To estimate the aggregate probability of a group (as defined above) being compromised, RMK uses Equation 8, which is based on Section 12 of (Lippmann, Riordan, Yu, & Watson, 2012).

$$P_{aggregate} = 1 - \prod_{i \in vulnerabilities} \left(1 - P_{compromise}(i)\right)$$

Equation 8: Estimated Aggregated Probability of Compromise

In the equation:

- $P_{aggregate}$ is the aggregate probability of compromise for the group.

- *vulnerabilities* is the set of all open vulnerabilities for each device in the group.
- $P_{compromise}$ is the probability of compromise for an individual vulnerability, as defined in Section 2.3.

3.2 Aggregate Impact

The aggregate impact is simply the arithmetic mean of the impact sub-score for each vulnerability in the group.

4 Interoperability with Other Systems

4.1 STIG

A STIG finding has only a one-dimensional category, which corresponds to the RMK impact sub-score (re-used from CVSS). The mapping from STIG finding categories to RMK severity levels is defined in Table 7.

STIG Category	STIG Severity	RMK Impact Sub-score
CAT I	High	7
CAT II	Medium	5
CAT III	Low	3

Table 7: Mapping from STIG Category to RMK Severity

To calculate the RMK composite impact score, combine the RMK impact sub-score (from the mapping in Table 7) with the CyTS (see Section 2.1.2) per Equation 1 in Section 2.1.3.

Unlike CVSS and some other methodologies, the STIG methodology does not have a separate exploitability dimension. Therefore, RMK also uses the mapped impact sub-score value from Table 7 as the exploitability sub-score (*Exploitability* in Section 2.2.1 and Equation 2**Error! Reference source not found.**). This is then combined with other factors per Section 2.2**Error! Reference source not found.** to calculate the final RMK exploitability score.

5 Future Work

5.1 CVSS 3.0

As noted in Section 1.2, this work is currently integrated with CVSS 2.2. A future revision will integrate with CVSS 3.0 while retaining backward compatibility with CVSS 2.2.

6 Works Cited

Defense Information Systems Agency. (2014, December 4). CMRS Risk Scoring 101. Fort Meade, Maryland.

Defense Information Systems Agency, Cybersecurity Range Branch (RE22). (2015, November 23). DISA Cyber-Terrain Scoring Rubric. Fort Meade, Maryland, USA.

Forum of Incident Response and Security Teams. (2007, June 20). *CVSS v2 Archive.* Retrieved November 8, 2015, from Forum of Incident Response and Security Teams: https://www.first.org/cvss/v2

Lippmann, R., Riordan, J., Yu, T., & Watson, K. (2012). *Continuous Security Metrics for Prevalent Network Threats: Introduction and First Four Metrics.* Lincoln Laboratory, Massachusetts Institute of Technology, Lexington.

Magnotti, L. (2015, January 8). *Is antivirus software still relevant?* Retrieved December 7, 2015, from Government Computer News: https://gcn.com/articles/2015/01/08/antivirus-software-still-relevant.aspx

United States Cyber Command. (2014, October 20). *Joint Enterprise Risk Assessment Model User Guide.* Retrieved September 20, 2015, from https://www.cybercom.smil.mil/j3/shared_/jeram%20guideline.pdf