Assessing Cybersecurity Risks

By Thomas M. Smith, CD, CISSP

September, 2022

ABSTRACT

In today's cyber threat environment, any organization is susceptible to security risks arising from the plethora a of threats, some real and some not so real. In any case, an organization would do well to perform risk assessment with a view to understanding the business impacts to the organization. An organization should also take into account risks associated with privacy, legal and regulatory, as well as contractual obligations.

This paper sets out the basic components of a risk assessment that can be adopted to perform a general high-level cybersecurity risk assessment using the guidance in the *Government of Canada (GC) Harmonized Threat and Risk Assessment (HTRA)* methodology.

Introduction

Any business should recognize that there are both risks and rewards in developing business opportunities and delivering services to clients. Certain risks are considered acceptable as long as they are adequately managed. Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues that may adversely affect business opportunities and services.

Information security means the preservation of confidentiality integrity and availability of information and therefore an information security risk assessment focuses on adverse events that could affect the preservation of these values. To determine the actual values an assessment is necessary using a systematic approach.

Using the HTRA methodology, risk (R) may be described as a functional relationship amongst asset values (AVal), threats (T) and Vulnerabilities (V):

$$R = f\,(AVal, T, V)$$

The values assigned to assets have a direct impact on calculating the risk levels. The asset values are expressed in terms of their confidentiality (C), integrity (I) and availability(A) ratings which are derived from a determination of the injuries that might reasonably be expected to arise in the event of a compromise to the C, I, or A of each critical asset.

A threat or threat agent can usually exploit flaws or inherent weaknesses in systems or applications, these are the main vulnerabilities and usually detected by vulnerability scanning software tools.

The approach to identifying the A_{val}, threats and vulnerabilities is consultative in nature. Business and program owners should be consulted to ascertain the potential impacts or injuries arising from a potential compromise and thereby influence the ratings for key assets such as information or services. In addition, any specific security concerns or other issues should be addressed as part of the threat and/or vulnerability assessment.

HTRA Processes Overview

Threat Assessment:

The need to determine the overall threat level is identified in the applicable HTRA methodology guidance. In particular, the value assigned to each relevant threat is necessary to calculate the overall risk level. The two key components that must be evaluated are the likelihood of the threat actor or threat event succeeding and the potential gravity or impact should the event be successful.

1. **Threat Likelihood:** determining the threat likelihood is based on past frequency of such events as well as the location of the events. Threats may have taken place in other similar organizations with similar sensitivity assets or in the same organization.
2. **Threat Impact:** the impact or gravity of a threat event is a measure of the amount of damage or the extent of compromise that is likely to arise should it occur. When considering deliberate threats, the capabilities of threat agents, in terms of knowledge, skills and resources, are sound indicators of the expected outcome.

The HTRA Methodology document provides detailed metrics that can be used to calculate each of the TA components noted above.

Vulnerability Assessment

It is necessary to identify and quantify vulnerabilities to effectively calculate risk levels using the formula. In general, all vulnerabilities contribute to risks in one or more ways such as:

- Attributes of some vulnerabilities increase the probability that a threat event will actually occur;
- Certain vulnerabilities increase the likelihood that a threat event will compromise an asset; and
- Other vulnerabilities allow threat events to cause even greater damage than that which might otherwise have been intended by the threat actor.

Prior to evaluating and rating any IT security related vulnerabilities, it is essential that existing or planned safeguards be considered as these can sometimes be effective measures in limiting an organization's exposure due to vulnerabilities that may exist within the IT environment being assessed.

When determining the vulnerability rating, there are two main contributors:

- **Probability of compromise:** effective preventive measures reduce the likelihood that a threat event will compromise an asset. Any vulnerabilities or inadequacies associated with these safeguards have the opposite effect, increasing the probability of unauthorized disclosure, destruction, removal, modification, interruption, or use of assets depending upon the nature of the threat.
- **Severity of outcome:** effective detection, response and recovery measures reduce the amount of damage arising from a compromising threat event. Any vulnerabilities or inadequacies associated with these safeguards have the opposite effect, increasing the severity, either the magnitude or the duration, of the unauthorized disclosure, destruction, removal, modification, interruption, or use of assets.

The HTRA Methodology document provides detailed metrics that can be used to calculate each of the VA components noted above.

Risk Analysis

The analysis of risks necessarily takes account of the assets susceptible to one or more threat actors as well as the vulnerabilities that may be exploited to gain access to the targeted assets.

The HTRA provides the following rating schema to calculate the cyber risks:

Qualitative A_V	Quantitative A_V	Qualitative T_L	Quantitative T_L	Qualitative V_R	Quantitative V_R
Very Low (VL)	1	VL	1	VL	1
Low (L)	2	L	2	L	2
Medium (M)	3	M	3	M	3
High (H)	4	H	4	H	4
Very High (VH)	5	VH	5	VH	5

After each component has an assigned value, the total value determines the risk level using the following:

Value Type	Risk Level				
Quantitative	1-4	5-15	16-32	36-75	80-125
Qualitative	VL	L	M	H	VH

When performing an analysis of the various threat actors and the potential or actual, vulnerabilities, the RA is usually limited to those plausible scenarios most likely to exist within the current operating environment and business rules for the application/system being assessed.

Summary

When assessing cyber risks, the HTRA methodology provides some flexibility in that it is intended to be scalable to handle all assets, physical and IT, both large and small, at an appropriate level of detail to satisfy business objectives. The methodology strives on its simplicity in that the underlying logic of the methodology must be intuitively satisfying and simply stated to permit easy application by program and project managers, as well as security practitioners. To enhance user-friendliness, the fundamental principles and processes of the harmonized methodology must be well illustrated with extensive charts, diagrams, examples, tables and templates.

Bibliography

1. *Government of Canada, Harmonized Threat and Risk Assessment (TRA) Methodology.*
2. *NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, Feb12, 2014.*
3. *Canadian Centre for Cyber Security (CCCS), Cloud Security Risk Management, March 2019.*
4. *Communications Security Establishment, Guide to Managing Security Risks from Using Information Systems, 31 March 2011.*
5. *Communications Security Establishment, IT Security Risk Management: A Lifecycle Approach, November 2012.*
6. *Communications Security Establishment, Information Systems Security Risk Management Activities, Annex 2, November 2012.*