Carnegie Mellon University
Software Engineering Institute

Loss Magnitude Estimation in Support of Business Impact Analysis

Daniel J. Kambic
Andrew P. Moore
David Tobar
Brett Tucker

December 2020

TECHNICAL REPORT
CMU/SEI-2020-TR-008
DOI: 10.1184/R1/13042955

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM20-0839

Table of Contents

List of Figures

List of Tables

Acknowledgments

We gratefully acknowledge the consulting support of CISA OCE, specifically Olga Livingston, Ph.D., Senior Economist, Office of the Chief Economist. Thanks also to Barbara White and Sandra Shrum for their excellent technical editing.

Abstract

This report describes the initial results of a research project to develop a transparent estimation method. This method leads to greater confidence in and improved ranges for estimates of potential cyber loss magnitude. The project team refined the Cybersecurity & Infrastructure Security Agency, Office of the Chief Economist (CISA OCE) Business Impact Analysis (BIA) method to support this estimation approach, including identifying factors and forming questions to ask stakeholders to elicit input for the loss magnitude estimation process. The project team also characterized the context for using factor tree analysis to produce an executable model in support of the refined BIA method since it can be applied to future cybersecurity assessments.

1 Introduction

When conducting Business Impact Analysis (BIA) for a system, it can be useful to go beyond qualitative impact categories such as Low, Moderate, and High [NIST 2004] to gain a deeper understanding of the full potential for adverse impacts; when possible, it is most useful to state these impacts in dollar equivalents. The results of the analysis of adverse impacts should depict not just the types of impacts (e.g., financial, safety, privacy, mission), but also their potential magnitude.

In this report, we propose a BIA method designed to lead to greater confidence in and improved ranges[1] for estimates of potential loss. The method we propose is a refinement of CISA OCE's (Cybersecurity and Infrastructure Security Agency, Office of the Chief Economist) BIA method that estimates the magnitude of potential loss associated with the loss of a system's Confidentiality, Integrity, and Availability (CIA).

Our method produces estimates of *potential* losses, its focus is on the impact of cyber incidents. We do not explicitly consider the extent of threats in the estimate, nor do we consider the cybersecurity controls that constitute the organization's and system's defenses. However, we do consider other system characteristics we were able to determine to be within the scope of this project. We developed the concepts and approaches described in this report in support of, and in collaboration with, the CISA OCE to help improve its BIA method for estimating potential loss magnitude.

The data we reviewed for this project includes information about high-value assets (HVAs), as designated by Federal civilian executive departments and agencies [OMB 2018]. We identified system factors that we used to characterize the systems, including factors that can be used to estimate the magnitude of potential losses.

This report focuses on the factor tree analysis we used to identify factors and generate questions that elicit additional useful information. We used this information to develop more accurate loss magnitude estimates. Improved loss magnitude estimates, especially when expressed in financial terms, can help organizations set priorities for needed actions and build a business case for mitigating risks to their systems. In addition to refining the BIA method, we expanded its context of use by conceptually demonstrating the execution of the method.

[1] Where there is uncertainty about potential impacts, we provide a range of impacts for decision makers to consider. We recommend using an impact range based on the likely impact, at the 50th percentile, and a high impact, at the 75th percentile. When the range of potential impacts is particularly wide, we recommend also developing an estimate of very high impact, at the 95th percentile.

2 Method Design and Application Overview

Figure 1 places the contents of this report in context with the overall BIA loss magnitude estimation method. The current seven-step method that constitutes loss magnitude estimation in the BIA is shown in the right-most column. In this report, we focus on the two middle columns ("Method Design" and "Method Support"). Both columns hinge on the development and use of a *factor tree* to (1) identify loss magnitude estimation factors and (2) relate them to loss magnitude estimation calculations. The loss magnitude estimation questions based on these factors are the focus of the interaction between the BIA analysis team and the stakeholder organization.

This report describes factor tree development and the questions derived from it. A companion paper[2] describes the equations that underlie the factor tree and its use for re-examining how the BIA method is applied to one of the systems previously analyzed by CISA OCE.

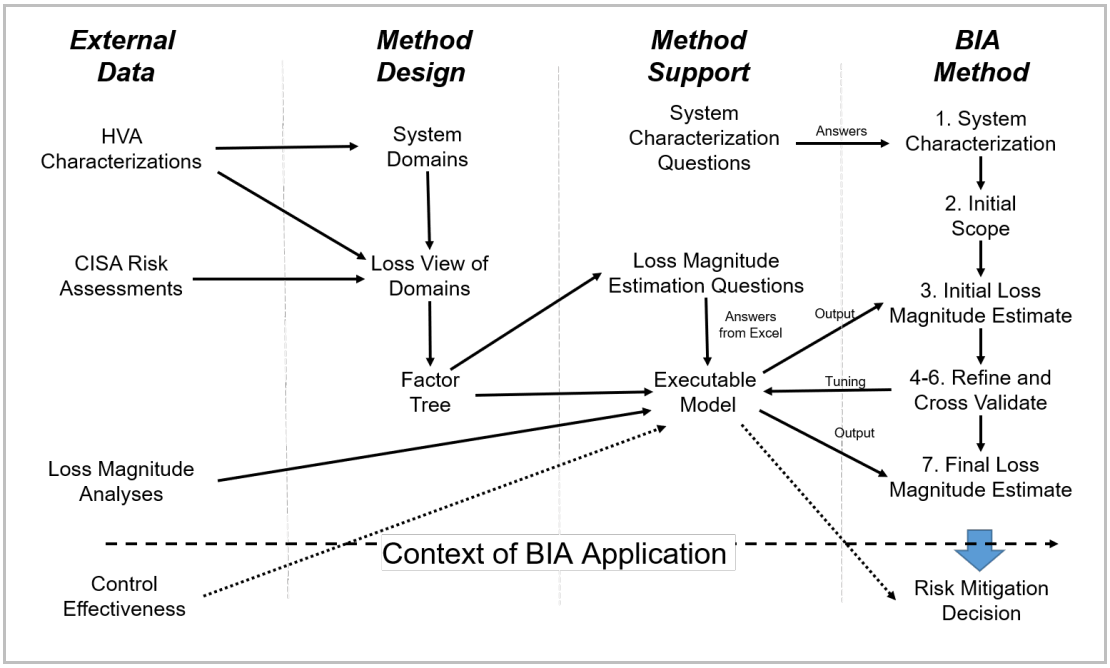


Figure 1: Method Design and Application Overview

[2] *Equations and Sample Calculations for Loss Magnitude Estimation in Business Impact Analysis: A Companion Report*. SEI limited distribution report. August 2020.

The Method Design column of Figure 1 shows that one of our inputs was information about HVAs in the Federal civilian executive government. We developed a system characterization approach (see Table 1) based on factors including "firmographics" (information about the organization the system supports), informational value (the extent to which the system processes sensitive information), domain, and impact. These characterization factors can be applied to HVAs or other systems of interest.

Table 1: System Characterization

	Factor
1	System ID
1a	System name
2	Firmographics
2a	System owner
2b	Organization type
2c	Number of employees in the organization/agency
2d	Number of employees in the business unit/department
2e	Total annual funding for the organization/agency (If industry, use revenue.)
3	Informational value
3a	Sensitive information: CUI, PII, PHI, LE, IP, pre-release sensitive, critical infrastructure
3b	For each type of sensitive information above: the specific quantity of information stored or processed
4	Domain
4a	Domain
4b	System mission: primary mission, mission support, or standard IT
4c	PMEF/MEF (only for Federal systems)
5	Impact
5a	FIPS 199 category
5b	Impact to the mission if unavailable for more than 12 hours
5c	Potential impact on regional or national health, public safety, and welfare of the U.S. (if industry, potential impact to the commercial viability of the organization)

Table 2 lists the domain elements of the characterization. We developed this domain list based on a review of the stated mission and purpose of each HVA system. Although the domains include a catch-all "Other" category, the list may be expanded as needed to cover groupings of additional systems of interest.

Table 2: System Domains

Domain	Description
Communications	Providing communications/broadcast capabilities (e.g., emergency, international networks)
Critical Infrastructure	Providing infrastructure services such as electricity, chemical processing, air travel and transportation, and postal delivery
Emergency Response	Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident; responding to natural disasters (e.g., wildfires, flood, volcano), including search and rescue
Finance	Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; providing financial and related systems (e.g., Social Security, taxes, financial aid, child support, securities, and economic data reporting)
Human Resources	Providing HR services, including payroll, benefits, jobs, personnel background checks, and clearances
Cyber & Information Technology	Providing all aspects of IT infrastructure and support (e.g., networks, databases, access management, FISMA reporting)
Law Enforcement	Enforcing the law, including areas such as counter drug trafficking, firearms, tracking defendants/offenders, bringing perpetrators of crimes to justice
Medical	Providing medical and health-related items (including VA medical support) as well as critical Federal Government services that address the national health
Safety	Providing critical Federal Government services that address the national safety and welfare needs of the United States (e.g., highway safety, food safety/tracking, air quality/radiation monitoring
Satellites & Space	Providing satellites and space systems
Security	Ensuring physical and personnel security and protecting against threats to the Homeland (e.g., border security, ICE, immigration, visa/refugee tracking)
Other	Providing other systems that do not neatly fit under previous categories (e.g., weather, patents and trademarks, labor relations)

We then developed *loss views* of the systems based on the system-specific properties reflected in the system characterization (Table 3). A *loss view* is a grouping of systems that have certain unique measures of loss associated with them. An example loss view is *Safety*; it applies to systems where an incident could cause injury or death. *Loss views are different from loss factors.*

A *loss factor* applies at a lower level of granularity that is not (necessarily) tied to a group of systems. It is relevant across all systems, except when the loss factor is unique to a loss view. As we analyzed systems for this project, we identified the four loss categories in Table 3 that identify unique measures for loss magnitude estimation. This is not an exhaustive list; with additional research, other loss views important to BIAs could certainly be proposed.

Table 3: Loss Views

Economic	Measures include unemployment costs and the costs of additional borrowing, including the potential increase in the cost of capital.
Environmental	Measures include the costs associated with environmental cleanup.
Financial	Measures include the direct theft of organizations' finances.
Safety	Measures include the loss of life and injury, using the value of a statistical life as a base measure.

Our work distinguishes the following elements from one another:

- systems themselves
- the domain associated with a system
- the loss factors associated with a system (or domain)
- the value that the loss factor takes on for a system

Many loss factors are relevant to all systems across all domains, for example, the costs associated with identifying that an incident has occurred and the evaluation of the extent of damage. The value of this loss factor is not the same across all systems and domains. But incident identification and evaluation should be considered when estimating loss magnitude across all systems and domains.

Conversely, some loss factors are not relevant to all systems, but only to a subset. For example, human safety is relevant only to systems in which an incident could cause death or injury to individuals internal or external to the organization the system supports. Identifying these system-specific loss factors is an important consideration when constructing the loss magnitude factor tree.

When building a factor tree, one goal is to "center" it on the factors that are common across all systems. System-specific factors must be addressed, but they are addressed primarily after the common aspects are addressed. This approach ensures that, to the greatest extent possible, the loss factors—and associated questions—apply across the greatest range of systems. Of course, system-specific loss factors and their associated questions must also be considered if they are relevant to the system being assessed.

Systems can have loss impacts that fall into multiple loss views, where loss considerations and associated questions apply. Table 4 shows key relationships among system domains and their potential loss impacts.

Table 4: System Domain to Loss View

Domain	Loss Views			
	Economic	Environmental	Financial	Safety
Communications	X		X	X
Critical Infrastructure	X	X	X	X
Emergency Response		X		X
Finance	X		X	
Human Resources	X		X	X
Information Technology	X	X	X	X
Law Enforcement		X		X
Medical	X		X	X
Safety		X		X
Satellites & Space	X	X	X	X
Security			X	X
Other	X	X	X	X

We developed a number of loss magnitude estimation questions based on system characterization and loss views. The stakeholder organization's answers to these loss magnitude estimation questions can come in the form of simple univariate averages (e.g., mode, median, or mean), but, if possible, should include as much univariate dispersion information as possible (e.g., standard deviation, quantiles, or ranges).

The BIA analysis team can import (e.g., from Excel) the documented answers into an executable model that helps conduct the analysis. The factor tree specifies the executable model by formally relating the loss magnitude estimation factors to the actual loss magnitude estimation. Figure 1, Step 3 of the BIA Method column shows the model's output is the initial loss magnitude estimates. Steps 4-6 perform refinements, adjustments, and cross validation to help tune the executable model and produce the final loss magnitude estimates in Step 7.

The executable model can also help the stakeholder organization use the loss magnitude estimates to evaluate how effectively risk mitigation controls are reducing its expected operational cybersecurity losses. In Figure 1, this evaluation is shown *below* the "Context of BIA Application" dotted line. We developed a prototype executable model to demonstrate this concept in support of the BIA method.

In Figure 1, the area *above* the "Context of BIA Application" line shows certain aspects that require continued effort. Analysis of CISA risk assessment data (specifically, Security Architecture Reviews) could provide a more granular and grounded view of the relationship between system characteristics and quantified loss than characterization information alone, even if monetizing the loss is not easy. In any case, using loss domains and factor trees as the basis for the BIA method might continue to be refined as CISA expands the number of systems that are assessed.

We narrowly focused our immediate work on improving loss magnitude estimations to possibly include them, if desired, in the BIA. The middle right portion of Figure 2 illustrates the focus of our current work in the overall decision-making context.[3]

Figure 2 depicts the path from loss magnitude estimation to the business case for organization leaders to consider when justifying cybersecurity decisions, including investments. The business case is formulated by comparing loss averted by a variety of cybersecurity controls with the cost of investing in those controls. Of course, the organization's leadership must make the ultimate decision. However, in this report, we do not consider the effectiveness of controls and associated loss averted in adopting those controls in refining the BIA loss magnitude estimation method, since they were outside the scope of our initial efforts. This effort focuses on improving the BIA method for calculating potential losses. The effectiveness of cybersecurity controls could be included in a future phase of this work.

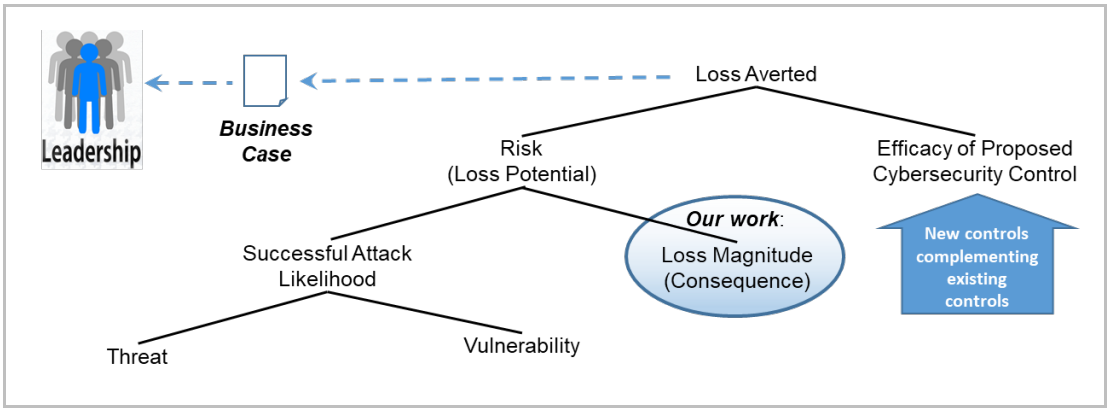


Figure 2: Analysis Context

[3] This depiction is consistent with the view of risk in Keeney and von Winterfeldt's article, "A Value Model for Evaluating Homeland Security Decisions" [Keeney 2011].

3 Method Design Approach

The factor tree analysis approach is thoroughly described in a paper by P. K. Davis and in associated Rand Corporation technical reports [Davis 2011]. We use this approach to identify factors then generate questions that elicit information needed to generate more accurate loss magnitude estimates. These estimates can help an organization's leaders build a business case for mitigating CIA risks to their systems. System dynamics modeling tools can be used to develop the factor tree.[4]

3.1 Factor Tree Method

Factors are incrementally broken down into subfactors, where a subfactor "tends to positively influence" the parent factor. When decomposing factors in one branch of the factor tree, an analyst generally assumes that factors considered in other parallel branches are out of the scope of their analysis.[5]

We use the loss view (Table 3) in our factor tree decomposition to identify system-specific concerns and their associated questions. While distinguishing system-specific concerns is important, we strive to orient as many factors as possible to be common among system types. The factor tree approach helps explain the important distinctions while identifying areas where factors can be abstracted and grouped with those common across system types. The goal is for questions to be as generally applicable as possible while ensuring that system-specific factors are identified. For example, internal factors such as lost productivity due to downtime should be addressed across all system types, whereas external factors involving loss of life due to downtime should be addressed only for systems that involve human safety. We also distinguish factors along CIA dimensions, where that distinction is important. Lost productivity is viewed primarily as an availability concern since it incurs downtime that inhibits personnel from working. The differences with regard to CIA and system type are indicated by color, as illustrated in Figure 3.

[4] We utilized the Vensim® tool. Vensim is a registered trademark of the Ventana Systems, Inc.

[5] In the original description of the factor tree method, factor trees are not necessarily trees, strictly speaking, in that a leaf node may be attached to multiple branches. We could, therefore, call these *factor diagrams* or *factor decompositions*, but to stay consistent with past usage, we adopt the original terminology.

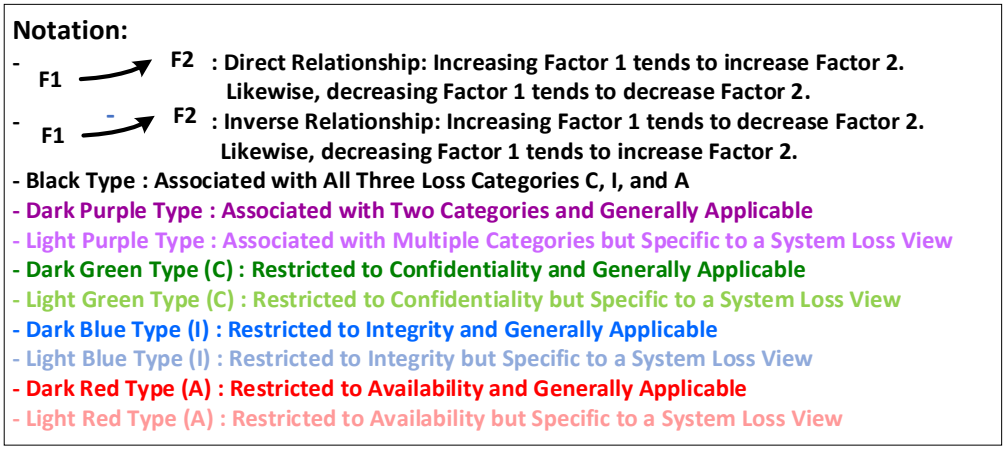


Figure 3: Factor Tree Notation

Sections 4 through 6 describe the factor tree incrementally; the full factor tree is depicted in the appendix. The mapping from factors to questions should be fairly straightforward, but we elaborate the questions incrementally with the factor tree for completeness.

3.2 Mapping Factors to Loss Magnitude Estimates

The factor tree we specify in this report, shown in full in the appendix, decomposes the factors involved in calculating loss due to cybersecurity compromise, distinguishing between the CIA areas. If the organization is primarily interested in losses due to a single factor, calculations can proceed in a fairly straightforward manner from the leaf node questions involving those factors to loss magnitude estimate calculations. However, as is common, organizations may be interested in multiple CIA factors. In that case, the estimation method must ensure that loss magnitude estimates do not double count factors that exist in more than one CIA branch.

Double counting is a particular concern when considering integrity and availability issues. The factor tree illustrates this concern in the symmetry of the decomposition in the factor tree along these two lines. It is important to consider integrity and availability separately since losses due to inaccessible data/services may involve different system characteristics than losses due to corrupted data/services. Also, corrupted data/services can be much more difficult to detect than inaccessible data/services.

Therefore, when considering both integrity and availability loss magnitude estimates, analysts must be very careful not to double count issues such as costs of consultation. The factor tree helps prevent double counting by identifying factors common among different CIA branches. When multiple CIA risks are applicable in a branch of the tree, and the organization is concerned about multiple CIA risks, the analyst must be wary of double counting costs associated with those factors. These concerns also pertain to confidentiality and the other factors. However, in the current instantiation of the factor tree, the only commonality is in the human safety domain. As the factor tree is refined and the number of loss domains represented in it increases, analysts must continue to scrutinize the data along these lines of commonality to prevent double counting.

4 Top-Level Loss Magnitude Estimation Factors

The top portion of Figure 4, above the root node (i.e., Potential Loss Magnitude), illustrates the loss factors common to all system types. The factors involved are all additive in nature at this level of abstraction.

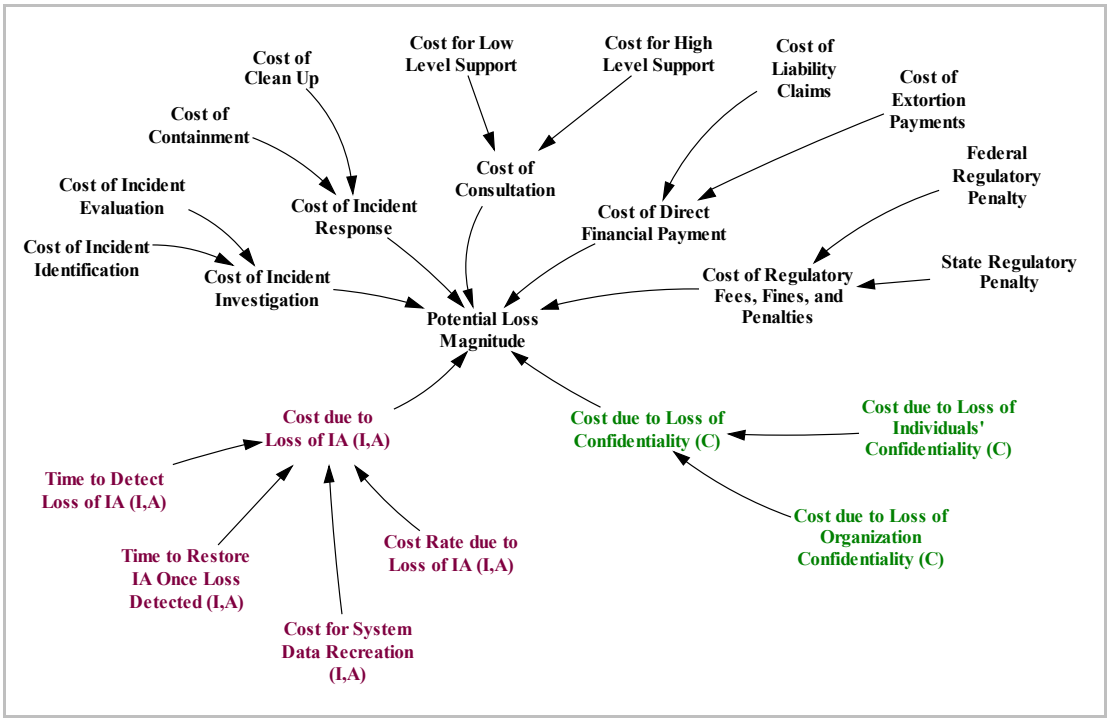


Figure 4: Top-Level Factor Tree for Potential Loss Magnitude

We elaborate on the "Cost of Consultation" and "Cost of Regulatory Fees, Fines, and Penalties" in the next sections. Aspects of incident response that include recovery and restoration are included in the factor decomposition branches below the root node. The other factors above the root node are not elaborated further in this report; however, general questions covering their intent include the following:

- What is the cost of the initial incident identification?
- What is the cost of evaluating the extent of compromise caused by an incident?
- What is the cost of containing the negative consequences of an incident?
- What is the cost of cleaning up the negative impacts of an incident?
- What is the cost of legal advice due to an incident?
- What is the cost of public relations due to an incident?
- What is the cost of federal regulatory fees, fines, and penalties resulting from an incident?
- What is the cost of state regulatory fees, fines, and penalties resulting from an incident?
- What is the maximum potential ransom payment that would be paid as a result of an incident?

The two factors below the root node in Figure 4 separate the cost of loss of integrity and/or availability (IA) from the costs of loss of confidentiality (C). The decomposition of these factors differs

when considering different system loss views. The decomposition also involves some factors that are specific to CIA.

While we discuss these factors in detail in the following sections, the cost of the loss of IA is calculated as follows:

Cost due to Loss of IA =
    Cost for System Data Recreation
    + (Time to Detect Loss of IA + Time to Restore IA Once Loss Detected)
      * Cost Rate due to Loss of IA

Cost of Loss of Confidentiality is simply the sum of the Cost of Loss of Individual's Confidentiality and the Cost of Loss of Organization Confidentiality.

4.1 Cost of Consultation

Consultation costs involve costs associated with legal guidance, public relations, media attention, and other management efforts related to incident response and recovery. These costs involve the number of hours spent and the cost per hour, which are both split by the low/high level in the organizational hierarchy of the personnel resources involved, as shown in Figure 7. The overall duration of the consultation sets the scope of the consultation costs.

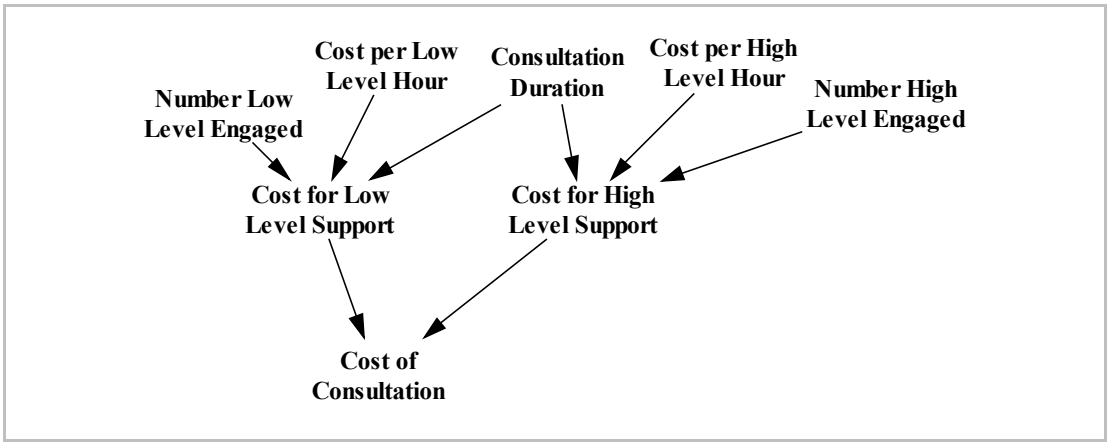


Figure 7: Cost of Consultation

Relevant questions include the following:

- How many low-level personnel are involved with public relations, media attention, or other incident response management?
- What is the hourly burdened rate of these low-level personnel?
- How many high-level personnel are involved with public relations, media attention, or other incident response management?
- What is the hourly burdened rate of these high-level personnel?

4.2 Cost of Regulatory Fees, Fines, and Penalties

Organizations may be subject to regulatory fees, fines, and penalties at both federal and state levels. For example, fines at the federal level may come from the Health Insurance Portability and Accountability Act (HIPAA) or the Securities and Exchange Commission (SEC). Many states have (or are considering) legislation that assesses fines on organizations per consumer per violation for unintentional disclosure. An example is the California Consumer Protection Act (CCPA). Such fines may become a major source of loss to organizations that suffer a data breach of individuals' personal information.[6]

Figure 8 shows the variables used in this calculation. Relevant questions include the following:

- How many individuals' records are at risk of compromise? (C)
- What federal fees, fines, or penalties may be assessed for information compromise (e.g., due to HIPAA or SEC regulations)?
- What fraction of records includes information about individuals residing in states that assess fees, fines, or penalties as a result of a confidentiality breach (e.g., California via the CCPA)? (C)

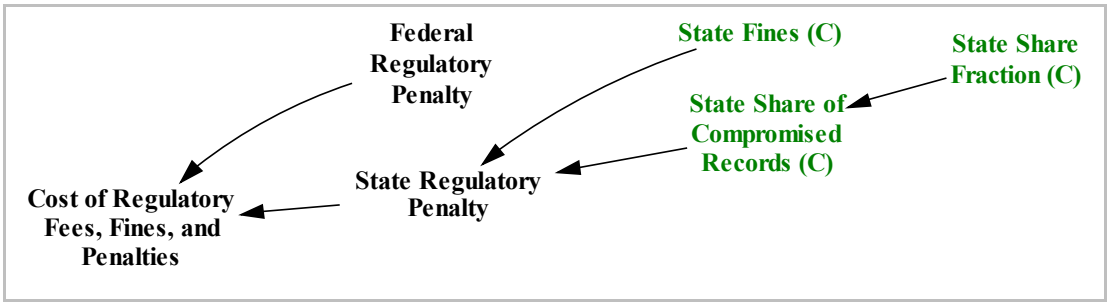


Figure 8: Cost of Regulatory Fines

[6] Some state fees, fines, and penalties such as CCPA do not apply to U.S. Federal Agencies. We include them here as a potential source of loss for other organizations, as applicable.

5 Time-Based Factors for Loss of Integrity/Availability

5.1 Time to Detect Loss of Integrity/Availability

A loss of integrity and or availability can manifest as either partial data corruption (an integrity issue) or complete inaccessibility (an availability issue). These distinctions are seen in Figure 5 in the first-level decomposition in both color and parenthetically at the end of the factor name—(I) for integrity and (A) for availability. A loss of integrity is often more subtle than a loss of availability; thus, it can be substantially more difficult to detect than a loss of availability. That is why integrity and availability are separated in parts of Figure 5—to promote probing questions related to those distinct possibilities.

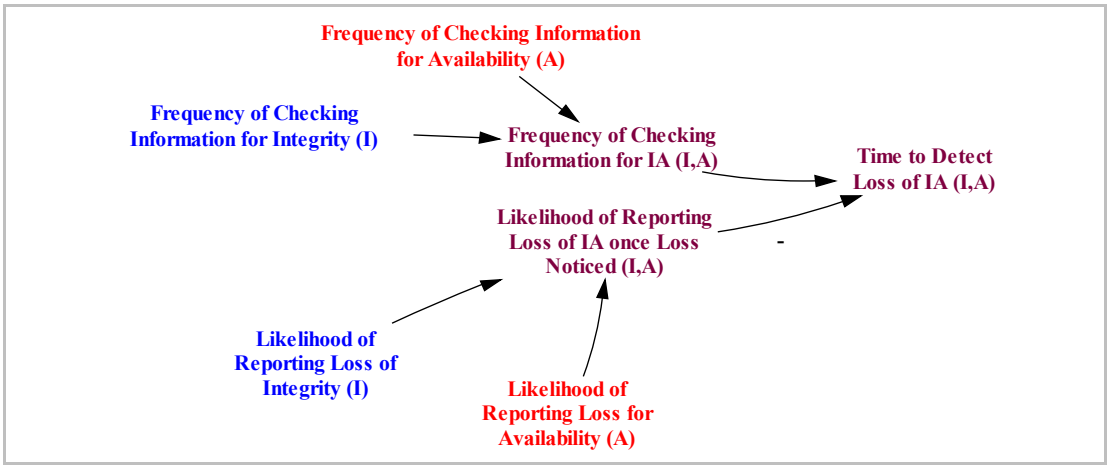


Figure 5: Time to Detect Loss of IA

Detecting a loss of IA depends on the frequency of use or other checking on the integrity and availability of the service or data. Automated checks ensure quick identification; without that identification, detection depends on reporting from individuals who rely on services/data.

Relevant questions include the following:

- How long does it take to detect a loss of information integrity or availability? (IA)
  - How long does it take to detect that data or services are corrupted? (I)
    - How soon after data or services become corrupted would the corruption be noticed? (I)
    - What is the likelihood that the corruption of data or services would be reported through an official channel after being noticed? (I)
  - How long does it take to detect that data or services are inaccessible? (A)
    - How soon after data or services become inaccessible would it be noticed? (A)
    - What is the likelihood that inaccessible data or services would be reported through an official channel after being noticed? (A)

5.2 Time to Restore Integrity/Availability Once Loss Detected

In this branch of the decomposition, shown in Figure 6, we assume the loss of IA has been detected and the question is how long will it take to restore the data and/or services to their previous state. Just as before, restoring a corrupted service could take longer than an inaccessible service if the exact nature of the corruption is difficult to ascertain (i.e., the service itself is accessible, but the integrity of accessed data could still be compromised). Even worse, the corruption could extend through previous backed-up versions of data if it was not detected in them.

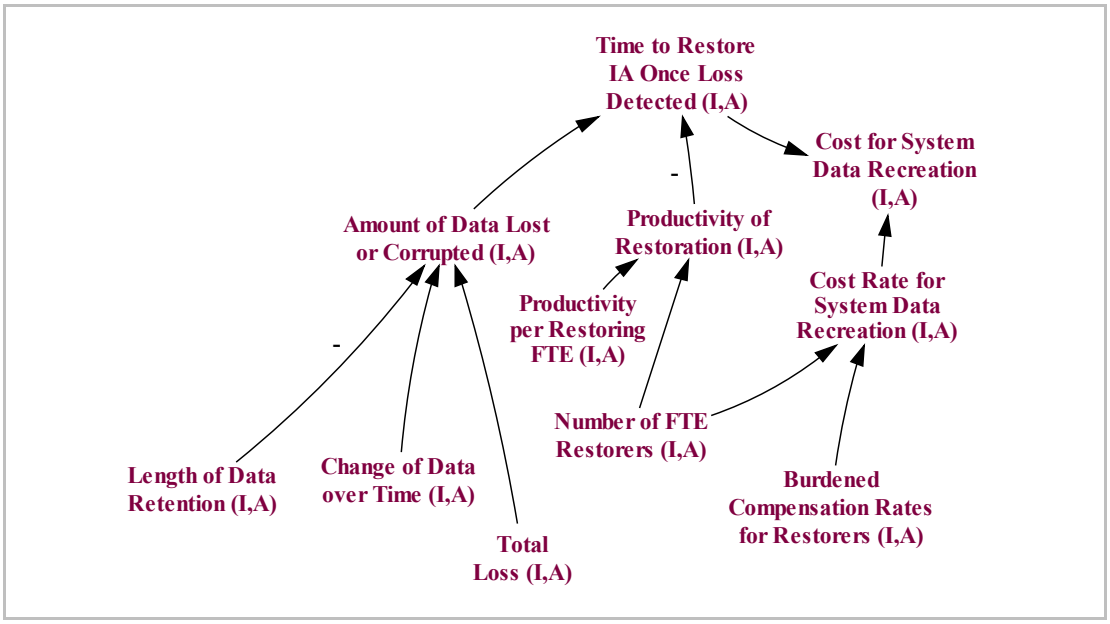


Figure 6: Time to Restore IA Once Loss Is Detected

The time to restore the data depends on the amount of data lost or corrupted (given the amount of data recoverable from backup) multiplied by the productivity of restoration. The amount of data lost or corrupted depends on the length of time backup data is retained and the change in the data compromised from the onset of the incident. We assume that any changes to the data after the incident occurs are unreliable. Of course, if data is not retained long enough or if backups are not made frequently enough, recreating the compromised data will take longer. The speed of the restoration depends on the productivity per resource assigned to the restoration task and the number of those resources. The cost rate for recreating system data also depends on the burdened compensation rates of the restorers.

Questions relevant for this portion of the factor tree include the following:

- How long does it take to restore information integrity and/or availability loss once it is detected? (IA)
  - How long does it take to restore access to services/data once its inaccessibility is detected? (A)
  - How long does it take to restore the integrity of service/data once its corruption is detected? (I)
    - How long are data and services backups retained? (IA)
    - How fast do data and services change over time? (IA)

        - How many full-time equivalents (FTEs) are assigned to restore data and services once inaccessibility or corruption is detected? (IA)
        - What is the productivity per FTE assigned to restore data and services once inaccessibility or corruption is detected? (IA)
- What is the cost rate for system/data recreation? (IA)
    - What is the burdened compensation rate for data/service restorers? (IA)

6 Cost Rate Factors for Loss of Integrity/Availability

Costs due to disruption can be split into two branches: internal and external; both types of costs are additive. Internal costs are those associated directly with the organization's operation, including cybersecurity efforts. External costs are those associated with impacts external to the organization. This section describes these two branches.

6.1 Internal Cost Rate Due to a Loss of Integrity/Availability

As seen in Figure 7, internal cost rates derive from two primary sources: lost revenue and lost productivity of internal staff who depend on the service and/or data for their job performance. Lost revenue often occurs in systems that involve authorization or approvals since they can involve fees to individuals seeking authorization (e.g., visa-application systems). Calculating lost productivity, which is often an issue when systems become unavailable, requires information about how many employees are affected by the outage, the percentage reduction in productivity resulting from the outage, and their burdened compensation rates.

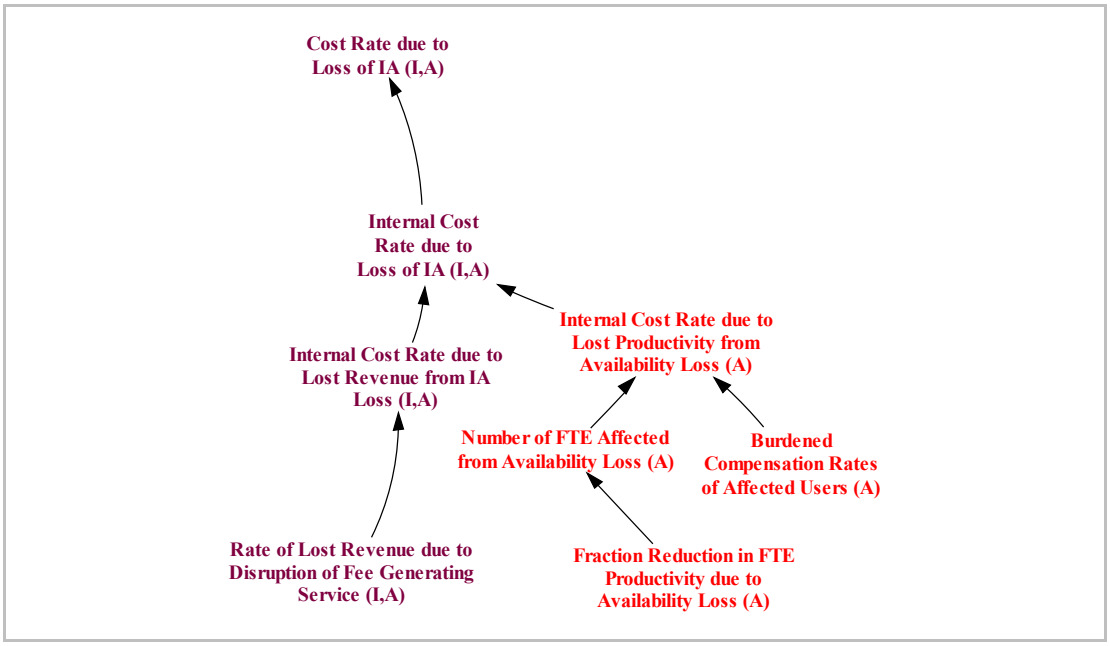


Figure 7: Internal Cost Rate Due to Loss of IA

Relevant questions include the following:

- What is the revenue loss rate from the IA loss? (IA)
- What is the rate of lost revenue from the disruption of a fee-generating service? (IA)
- What is the rate of lost productivity from Availability loss? (A)
- What is the number of FTE affected by inaccessible services or data? (A)
- What is the percentage reduction of productivity due to inaccessible services or data? (A)
- What is the burdened compensation rate of the affected users? (A)

6.2 External Cost Rate Due to a Loss of Integrity/Availability

Regarding external costs, the factors break down by system loss view as shown by the factors in light purple, light red, and light blue in Figure 8. The loss-view specific factors, introduced in Table 3, are elaborated as follows:

- **Economic**. Economic costs include costs related to job loss and additional borrowing and potential increases in the cost of capital. Additional borrowing may be due to external impacts of loss of financial support due to system downtime.
- **Environmental**. Environmental costs include environmental and property damage cleanup costs.
- **Financial**. Financial costs occur directly from theft or fraud that happen as part of the disruption or as a result of financial credit needed by those affected by the disruption. Theft occurring due to the corruption of information may result in increased payouts to authorized individuals or accounts diverted to malicious individuals (or their friends and family). Financial costs may also include losses due to the financial credit needed by individuals experiencing a disruption of payouts.
- **Safety**. The human safety domain calculates cost based on the death of or injury to people. The number of deaths or injuries can be roughly valued using the government's set value of a statistical life [DOT 2016]. Other allowable costs of injury include costs of lost productivity until the injured party recovers full function and disability claims that result from a complete loss of the ability to function at work.

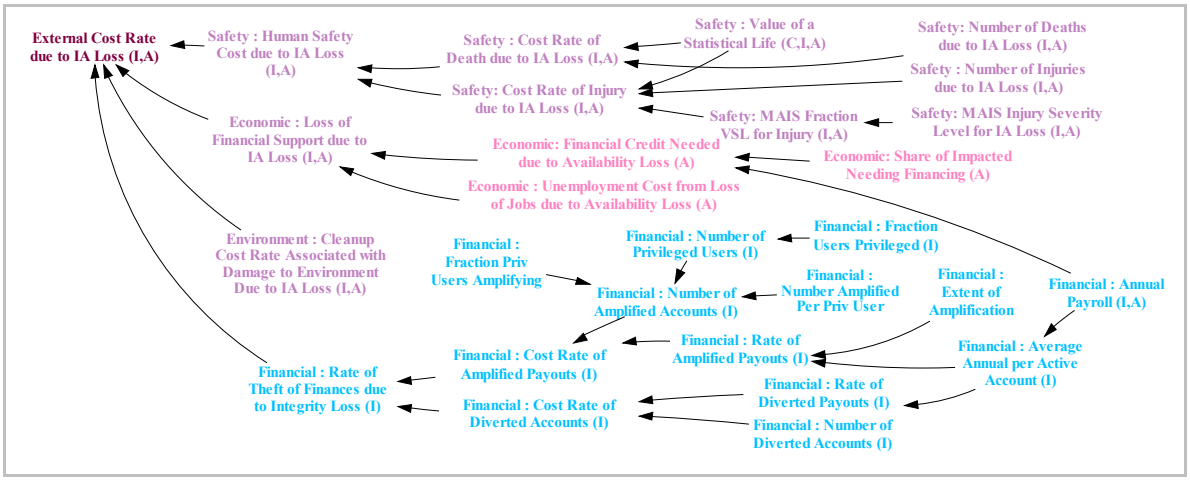


Figure 8: External Cost Rate Due to IA Loss

Relevant questions include the following:

For the Safety View

- What death rate will result due to inaccessible services or data? (A)
- What death rate will result due to corrupted services or data? (I)
- What injury rate and severity will result due to inaccessible services or data? (A)
- What injury rate and severity will result due to corrupted services or data? (I)

For the Economic View

- What is the annual payroll for the organization? (A)
- What are the costs of employee credit needed as a result of Availability loss? (A)
- How many unemployment claims will result due to Availability loss? (A)

For the Environment View

- What are the environmental damage cleanup costs that will result from loss of IA? (IA)

For the Financial View (Payroll Systems in Particular)

- How many active payroll accounts are supported? (I)
- What is the annual payroll supported by the system? (I)
- What is the pay period? (IA)
- How many privileged users have accounts on the system (i.e., users that can add or alter payroll information)? (I)
- What level of increased payout is possible without triggering additional checking or alerting? (I)

6.3 Cost Due to Loss of Confidentiality

As shown in Figure 9, the costs of a loss of Confidentiality break out into whether the loss involves a disclosure of the organization's information versus an individual's information that was entrusted to the organization. In the latter case, breach laws require notification and remuneration of the credit-monitoring costs to the victims. Victim response costs to the organization depend on the number of individuals affected[7] and the type of information lost. Historically, costs due to a loss of Protected Health Information (PHI) are greater than a loss of PII, so these will likely require different considerations for loss magnitude estimates [Coburn 2019].

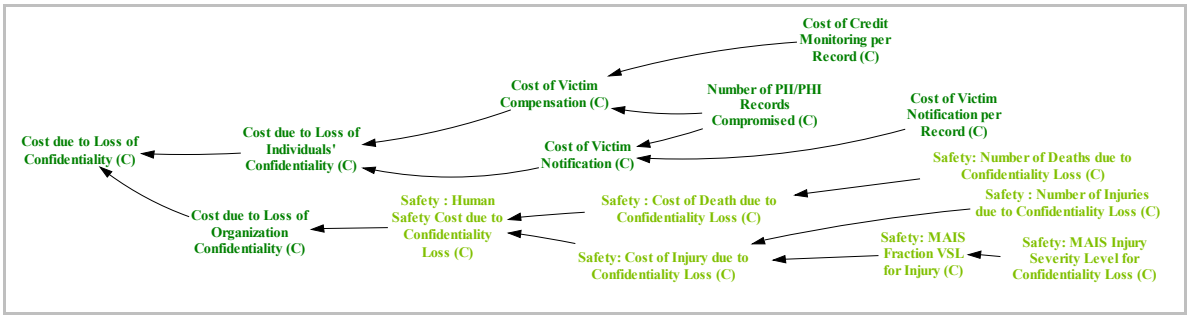


Figure 9: Cost Due to Loss of Confidentiality

While costs due to the disclosure of other sensitive organizational information is difficult to quantify, for the human safety domain, disclosures can compromise the identity of government

[7] Traditional approaches that use a single cost-per-record metric for loss estimates tend to underestimate the cost of small events and overestimate large events. Cyentia Institute published its study in 2020 [Cyentia 2020].

personnel, even undercover agents, and result in the death or injury of those personnel. The monetization of this potential loss was discussed in the previous section.

Relevant questions include the following:

- How many individuals' PII is at risk of unauthorized disclosure? (C)
- How many individuals' PHI is at risk of unauthorized disclosure? (C)
- What is the cost of victim notification per number of victims notified? (C)

For the Safety View

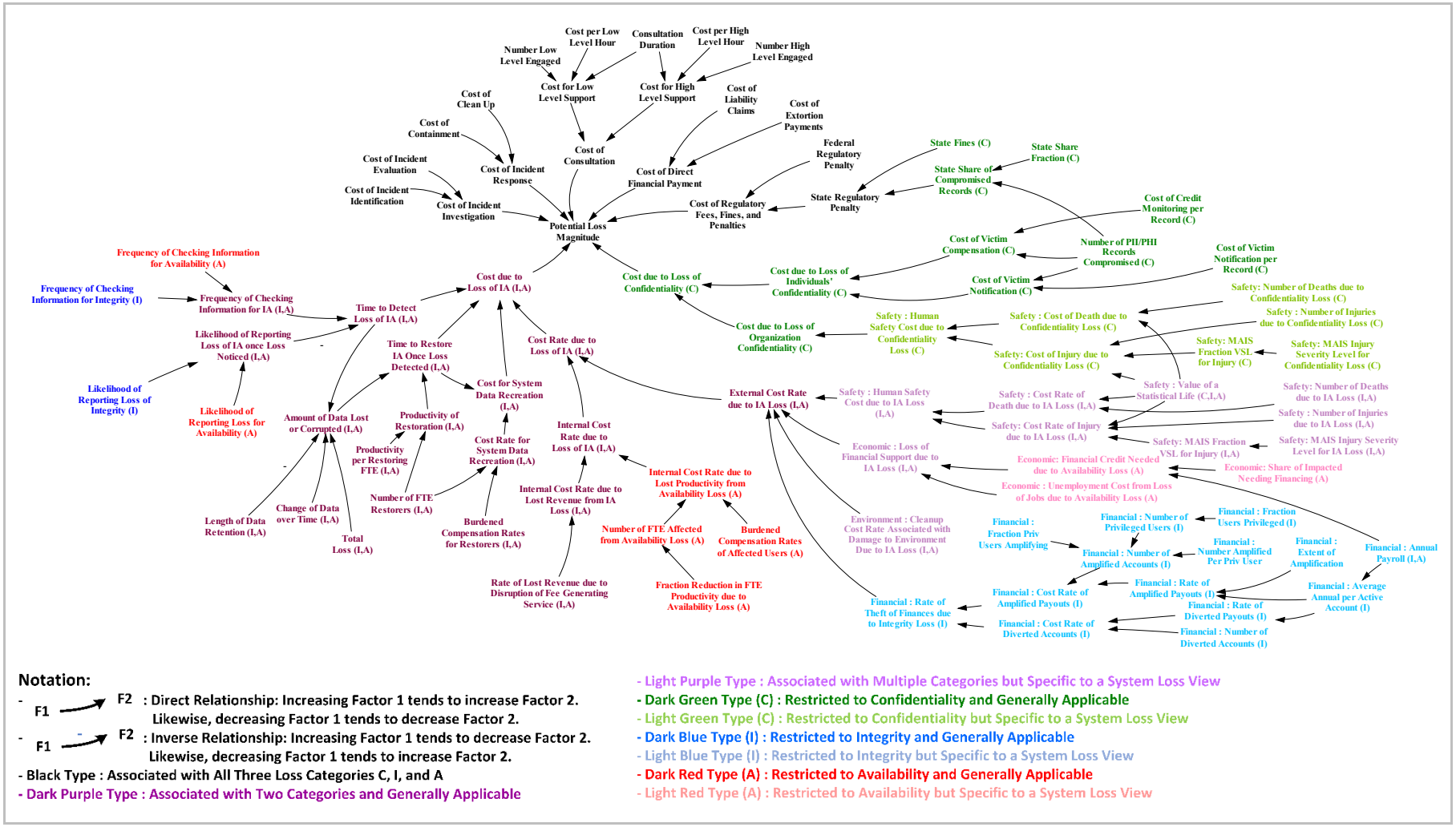
- How many deaths will result due to a loss of confidentiality? (C)
- How many injuries will result due to a loss of confidentiality? (C)
- What is the severity of each of the injuries that will result due to loss of confidentiality? (C)

7 Conclusion

This report describes the initial results of a research project proposing a transparent estimation method designed to lead to greater confidence in and improved ranges for estimates of potential loss magnitude. We refined the CISA OCE BIA method to support this approach, including identifying factors and questions to ask stakeholders that help elicit the needed information as input to the loss magnitude estimation process. We also characterized the context for using factor tree analysis to produce an executable model in support of the refined BIA method since it can be applied to future cybersecurity assessments.

We recommend conducting additional research to refine and update factor tree inputs to the executable model as information becomes available and extend the use of the model for risk mitigation decision support. This research can include developing an extended review of factors noted as relevant to losses in recent cyber-loss reporting. As part of the research, we recommend conducting sensitivity analysis on these factors to understand which are key to the highest potential losses and which have potential for extensive growth. In addition, a separate review of Security Assessment Reports (SARs) and their responses would help determine which types of systems are underrepresented in the assessment history.

Appendix: Potential Loss Magnitude Factor Tree



References

URLs are valid as of the publication date of this document.

[Coburn 2019]
Coburn, A.; Leverett, E.; & Woo, G. *Solving Cyber Risk: Protecting Your Company and Society*. Wiley, 2019. ISBN: 978-1-119-49092-0. https://b-ok.cc/book/3658057/f725b5

[Cyentia 2020]
Cyentia Institute. *Information Risk Insights Study*. 2020. https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf

[Davis 2011]
Davis, P. K. "Primer for Building Factor Trees to Represent Social Science Knowledge." *Proceedings of the 2011 Winter Simulation Conference*. 2011. http://www.informs-sim.org/wsc11papers/277.pdf

[DOT 2016]
U. S. Department of Transportation (DOT) *Guidance on Treatment of the Economic Value of a Statistical Life (VSL) in U.S. Department of Transportation Analyses – 2016 Adjustment* (Memorandum). August 8, 2016. https://www.transportation.gov/sites/dot.gov/files/docs/2016%20Revised%20Value%20of%20a%20Statistical%20Life%20Guidance.pdf

[Keeney 2011]
Keeney, R. L. and von Winterfeldt, D. "A Value Model for Evaluating Homeland Security Decisions." *Risk Analysis*. Volume 37. Number 9. March 2011. https://doi.org/10.1111/j.1539-6924.2011.01597.x

[NIST 2004]
National Institute of Standards and Technology (NIST). *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems*. 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[OMB 2018]
Office of Management and Budget (OMB). *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program* (Memorandum M-19-03). December 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	December 2020	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Loss Magnitude Estimation in Support of Business Impact Analysis	FA8702-15-D-0002

6. AUTHOR(S)

Daniel J. Kambic, Andrew P. Moore, David Tobar, and Brett Tucker

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2020-TR-008

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report describes the initial results of a research project with the purpose of developing a transparent estimation method. This method is designed to lead to greater confidence in and improved ranges for estimates of potential loss magnitude. The project team refined the Cybersecurity & Infrastructure Security Agency, Office of the Chief Economist (CISA OCE) Business Impact Analysis (BIA) method to support this estimation approach, including identifying factors and formulating questions to ask stakeholders, to elicit input for the loss magnitude estimation process. The project team also characterized the context for using factor tree analysis to produce an executable model in support of the refined BIA method since it can be applied to future cybersecurity assessments.

14. SUBJECT TERMS	15. NUMBER OF PAGES
loss magnitude estimation process, cybersecurity assessments, BIA, eliciting input	29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL