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

September 2020

TECHNICAL REPORT
CMU/SEI-2020-TR-XXX

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

1 Introduction

In conducting a system Business Impact Analysis (BIA), it can be useful to go beyond qualitative impact categories such as Low, Moderate, and High[1] to gain a deeper understanding of the full potential for adverse impacts, stated in dollar equivalent terms when possible. Analysis of adverse impacts should depict not just the types of impacts (e.g., financial, safety, privacy, mission, etc.) but also their potential magnitude.

This report proposes a methodology that leads to greater confidence in and improved ranges[2] for estimates of potential loss. This methodology is a refinement of CISA OCE's (Cybersecurity and Infrastructure Security Agency, Office of the Chief Economist) BIA methodology of estimating the potential loss magnitude associated with loss of Confidentiality, Integrity, and Availability (CIA) of the systems being assessed. The estimate is of *potential* loss magnitude because we do not explicitly consider the extent of threat in the estimate, nor do we consider the extent of cybersecurity controls that constitute the organization's and system's defense. However, we do consider other characteristics of systems under assessment to the extent that we were able to determine them within the scope of this project. The authors developed the concepts and approaches described in this report in support of, and in collaboration with, the CISA OCE to help improve their BIA potential loss magnitude estimation methodology.

The data we accessed for this project involves characterizations of high value assets (HVAs), as designated by Federal civilian executive departments and agencies.[3] We identified a set of system factors that we used to characterize the systems, including factors that can be used to estimate the magnitude of potential losses. We used factor tree analysis to identify factors to generate questions that elicit additional useful information for developing 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 an economically justifiable business case for mitigating risks to their systems. In addition to refining the BIA method, we elaborated its context of use; we provide a conceptual demonstration of the execution of the method.

The authors gratefully acknowledge the consulting support of CISA OCE, specifically Olga Livingston, Ph.D., Senior Economist, Office of the Chief Economist.

---

1 National Institute of Standards and Technology. (2004). *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems*

2 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.

3 For additional information on high value assets see Office of Management and Budget Memorandum *M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, December 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

2 Method Design and Application Overview

Figure 1 places the contents of this report in context with the overall BIA loss magnitude estimation methodology. The current seven-step method that constitutes loss magnitude estimation in the BIA is shown in the right-most column of Figure 1. This report focuses on the two middle columns ("Method Design" and "Method Support"), which hinge on the development and use of a *factor tree* to identify loss magnitude estimation factors and relate those with the 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 the factor tree development and the questions derived from it. A companion paper[4] describes the equations that underlie the factor tree and its use to re-examine an application of the BIA method to one of the HVA systems previously analyzed by CISA OCE.

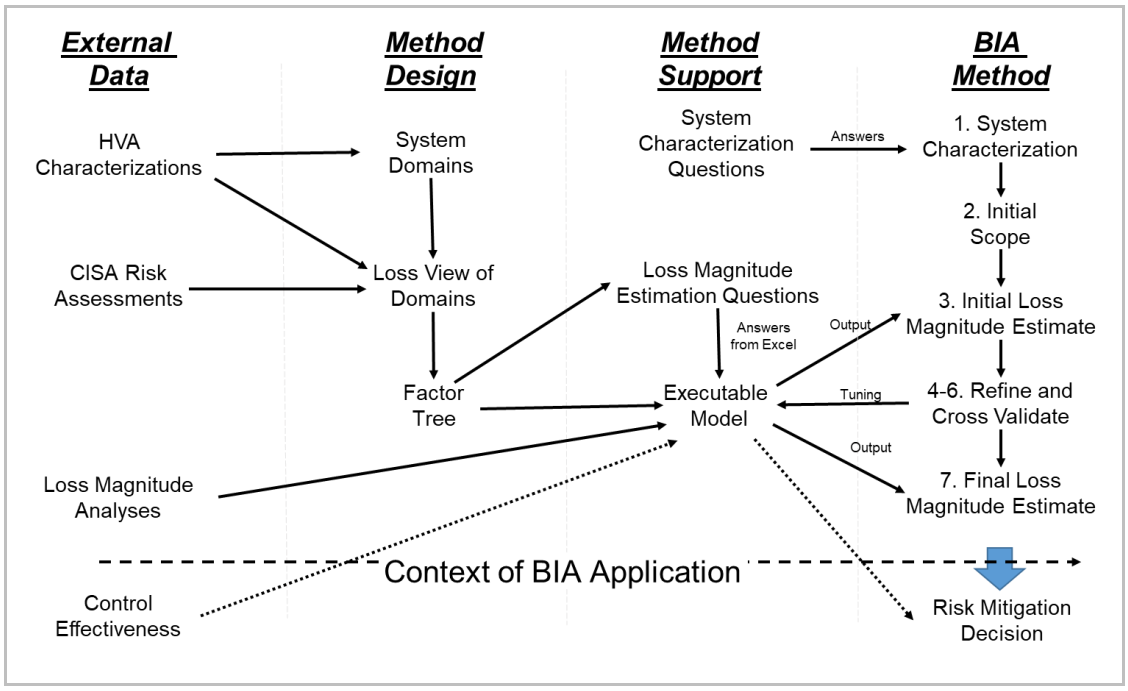


Figure 1: Method Design and Application Overview

As shown in the Method Design column of Figure 1, 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 a number of relevant factors, including "firmographics" (i.e., information about the

[4] "Equations and Sample Calculations for Loss Magnitude Estimation in Business Impact Analysis: A Companion Report." SEI report. August 2020.

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 organization/agency (If industry, use revenue)
3	Informational Value
3a	Sensitive Info: CUI, PII, PHI, LE, IP, Pre-Release sensitive, Critical Infrastructure
3b	For each type of sensitive info above, specific quantity of information stored or processed
4	Domain
4a	Domain
4b	System Mission: Primary Mission / Mission Support / Standard IT
4c	PMEF/MEF (only for Federal systems)
5	Impact
5a	FIPS 199 category
5b	Impact to mission if unavailable for greater than 12 hours
5c	Potential impact on regional or national health, public safety and welfare of the US (If industry, potential impact to commercial viability of organization)

Table 2 lists the domain element of the characterization. We developed this domain list based on a review of HVA systems' stated mission and purpose. 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	Communications/broadcast capabilities (emergency, international networks, etc.)
Critical Infrastructure	Representative examples include electricity, chemical, air travel and transportation, postal service, etc.
Emergency Response	Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident; responding to natural disasters (wildfires, flood, volcano), search and rescue

Finance	Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; finance and related systems (Social Security, taxes, financial aid, child support, securities, and economic data reporting, etc.)
Human Resources	HR, including payroll, benefits, jobs, personnel background checks and clearances
Cyber & Information Technology	All aspects of IT infrastructure and support, e.g. networks, databases, access management, FISMA reporting
Law Enforcement	Includes counter-drug trafficking, firearms, tracking defendants/offenders, bringing to justice perpetrators of crimes
Medical	Medical and health-related items (including VA medical support); critical Federal Government services that address the national health
Safety	Providing for critical Federal Government services that address national safety and welfare needs of the United States, e.g., highway safety, food safety / tracking, air quality / radiation monitoring
Satellites & Space	Satellites and space systems
Security	Physical and personnel security, protecting against threats to the Homeland (border security, ICE, immigration, visa / refugee tracking, etc.)
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 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, which applies to systems in which 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. Its relevance is common across all systems, except when the loss factor is unique to a loss view. From our analysis of systems of interest, we identified four loss categories that identify unique measures for loss magnitude estimation: economic, environmental, financial, and safety, presented in Table 3. This is not an exhaustive list; with additional research, other loss views important to BIAs will certainly come to light.

Table 3: Loss View

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

Our work distinguishes systems, the domain with which a system is associated, the loss factors associated with a system (or domain), and the value that the loss factor takes on for a specific 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 applies across all systems and all domains. That is not to say that the value of this loss factor is the same across all systems

and domains; the values will likely differ. But incident identification and evaluation is a factor to be considered in estimating loss magnitude across all systems and domains.

However, some loss factors are not relevant to all systems, but only to a subset of systems. For example, human safety is only relevant 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 in constructing the loss magnitude factor tree. One goal of our factor tree decomposition is to "center" the factor tree in the set of factors that are common across all systems. System-specific factors must be addressed, but they are addressed primarily after the common aspects have been addressed. This approach ensures that, to the greatest extent possible, the loss factors—and associated questions—apply across the greatest range of systems. System-specific loss factors and their associated questions must also be considered if they are relevant to the particular system being assessed.

Systems may have loss impacts that fall in multiple of these loss views, where case loss considerations and associated questions for all relevant impacts apply. Table 4 shows the relationship among the various system domains and their associated potential loss impacts.

Table 4: System Domain to Loss View

DOMAIN	LOSS			
	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 the system characterization and loss views. Answers to the loss magnitude estimation questions by the stakeholder organization can come in the form of simple univariate averages (such as mode, median, or mean), but, if possible, should include as much univariate dispersion information as possible (such as standard deviation, quantiles, or ranges). The answers can be documented and then imported (e.g., from Excel) into an executable model that could help the BIA analysis team conduct its analysis. The factor tree specifies the

executable model by formally relating the loss magnitude estimation factors to the actual loss magnitude estimation. The model's output serves as the initial loss magnitude estimates in Figure 1, Step 3 of the BIA Method column. The refinements, adjustments, and cross validation occurring in Steps 4-6 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 the effectiveness of risk mitigation controls for reducing their expected operational cybersecurity losses. This is shown below the "Context of BIA Application" dotted line in Figure 1; this aspect of the development was out of scope for our initial efforts. Nevertheless, we developed a prototype executable model to demonstrate the concept in support of the BIA method.

Certain aspects depicted above the "Context of BIA Application" line in Figure 1, while in scope, require continued effort. We were unable to gain access to CISA risk assessment data (specifically Security Architecture Reviews) as input to our analysis for this effort. Such data could provide a more granular and grounded view of the relationship between system characteristics and quantified loss than is possible with characterization information alone, even if monetization of the loss cannot easily be formulated. In any case, the loss domains and factor tree basis for the BIA method may continue to be refined as CISA expands the number of systems that are assessed.

Our immediate work is narrowly focused on improving loss magnitude estimations for their inclusion, if desired, in the BIA. The middle right portion of Figure 2 illustrates the focus of our current work in the context of an overall decision-making model.[5]

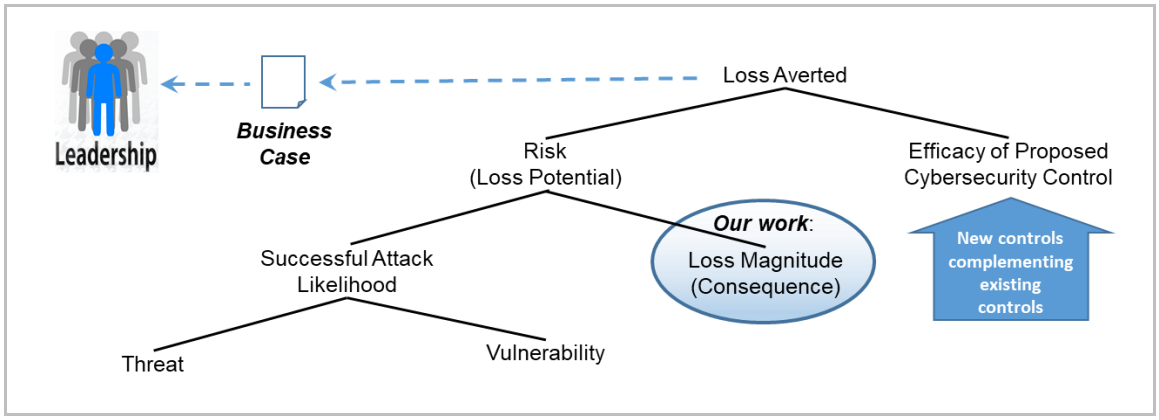


Figure 2: Analysis Context

Figure 2 depicts the path from loss magnitude estimation to the business case for organization leaders to consider in 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

[5] This depiction is consistent with the view of risk in Keeney and von Winterfeldt (2011). "A Value Model for Evaluating Homeland Security Decisions," *Risk Analysis*. Vol. 37, No. 9.

those controls. Of course, the ultimate decision must be made by the organization's leadership. However, in this report the effectiveness of controls and associated loss averted in adopting those controls are not considered in refining the BIA loss magnitude estimation method, since they were outside the scope of our initial efforts. This effort is focused specifically on improving the BIA methodology for calculating potential losses. The effectiveness of cybersecurity controls could be included in a future phase of this work.

3 Method Design Approach

The factor tree analysis approach is thoroughly described in a conference paper by P.K. Davies and in associated Rand Corporation technical reports.[6] We use this approach to identify factors to generate questions that elicit information needed to generate more accurate loss magnitude estimates. These estimates can help organization leaders build an economically justifiable business case for mitigating CIA risks to their systems. We use the Vensim® system dynamics modeling tool to develop the factor tree.

3.1 Factor Tree Methodology

Factors are incrementally broken down into subfactors where the relationship is that 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 scope of the analysis.[7]

The loss view (Table 3) is used in our factor tree decomposition as appropriate 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 to explain the important distinctions while also identifying areas where factors can be abstracted so as to be common across system types. The goal is for questions to be as generally applicable as possible while still 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 only need to be addressed for systems that involve human safety. We also distinguish factors along the CIA dimensions where that distinction is important. Lost productivity is viewed primarily as an availability concern since that incurs

---

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

® Vensim is a registered trademark of the Ventana Systems, Inc.

[7] 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.

downtime that inhibits personnel work. The differences with regard to CIA and system type are indicated by color, as explained in Figure 3.

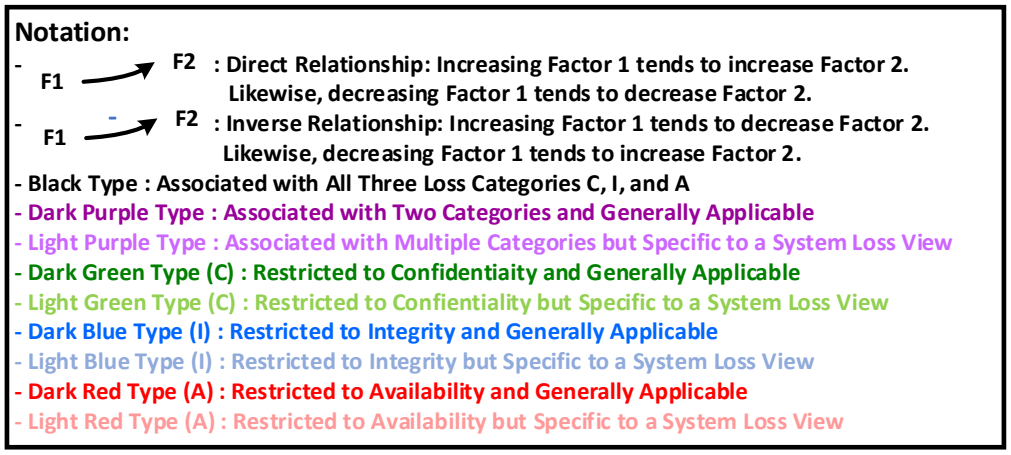


Figure 3: Factor Tree Notation

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 specified in this report, and as 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 of the 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 both integrity and availability issues, as is seen 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. 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 organization of the factor tree helps prevent double counting by specifying factors that are common among different CIA branches to the greatest extent possible. Whenever multiple of the 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 exist with confidentiality and

the other factors, but in the current instantiation of the factor tree the only commonality is in the human safety domain. Future refinement of the factor tree and the loss domains represented in it requires continued scrutiny along these lines of commonality to prevent double counting.

4 Top Level Loss Magnitude Estimation Factors

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

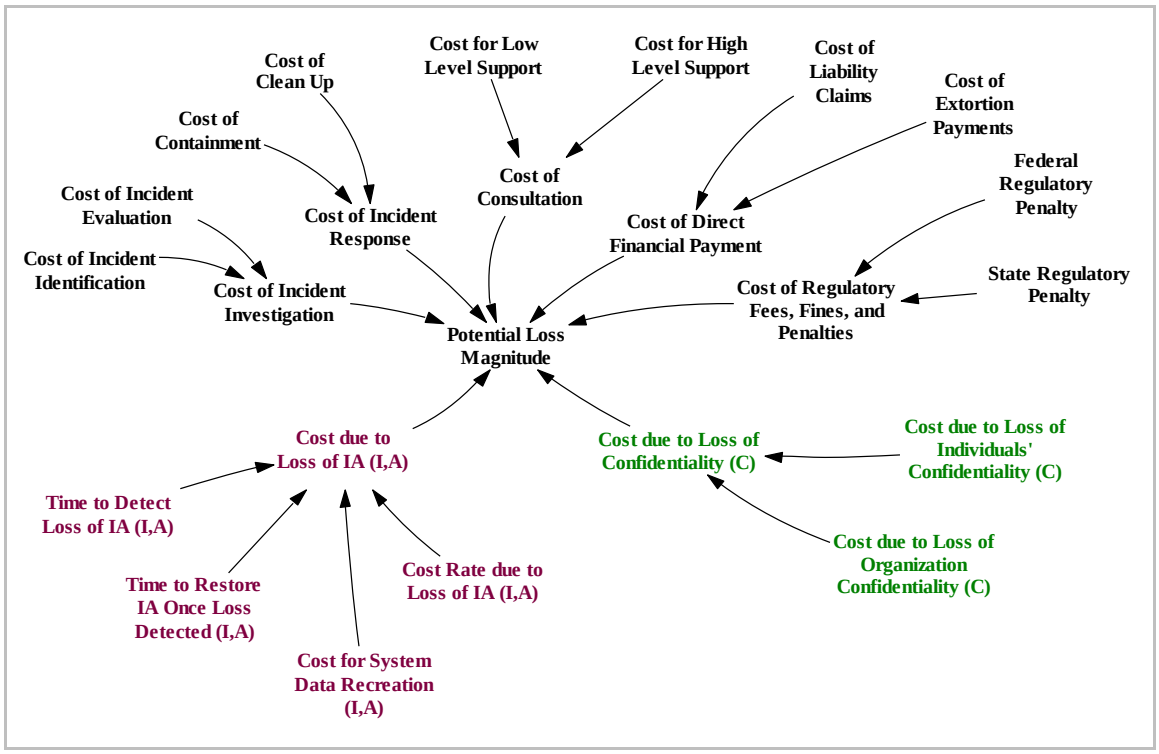


Figure 4: Top-Level Factor Tree for Potential Loss Magnitude

The "Cost of Consultation" and "Cost of Regulatory Fees, Fines, and Penalties" are elaborated 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 cost of loss of integrity and/or availability (IA) from costs of loss of confidentiality (C). The decomposition of these factors does differ some when considering different system loss views. The decomposition also involves some factors that are specific to CIA.

While these factors are discussed 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.

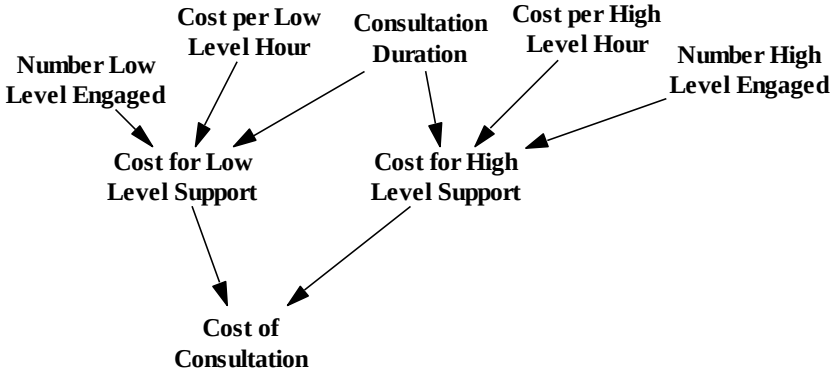


Figure 7: Cost of Consultation

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 a federal and a state level. For example, fines at a 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 suffering from a data breach of individuals' personal information.[8]

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)

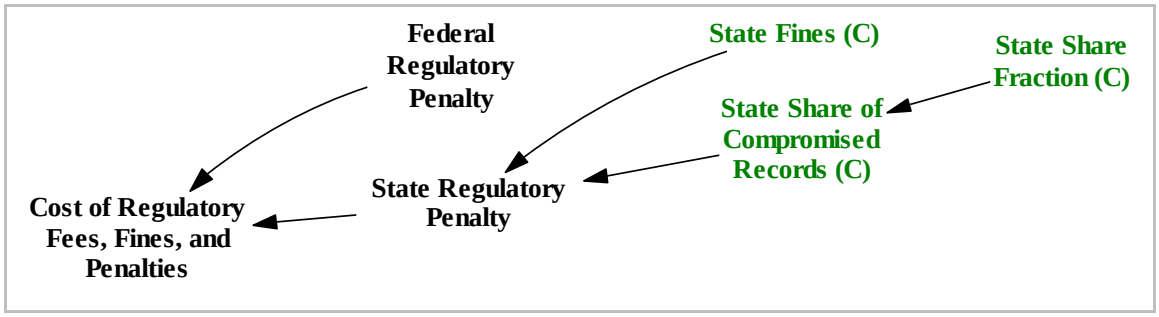


Figure 8: Cost of Regulatory Fines

[8] 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

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.e., I for integrity and A for availability). Detecting loss of integrity can be much more subtle, and thus substantially more difficult to detect than detecting loss of availability; therefore, it is separated in Figure 5 to promote probing questions related to those distinct possibilities.

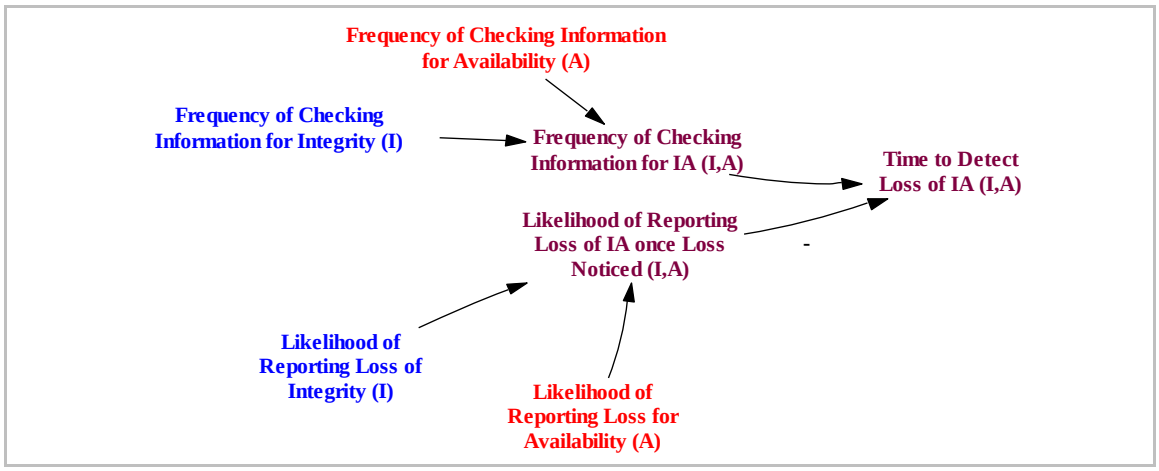


Figure 5: Time to Detect Loss of IA

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

Two possibilities in corrupted financial data are important:

1. First, a malicious agent may substitute their own or a colluder's name and address for the subject's name and address, for example to divert funds for financial/payroll systems or divert transaction approvals for authorization systems, such as visa application systems or clearance management systems.
2. A malicious agent corrupting the information associated with an authorized subject (e.g., the amount they are paid) can be just as damaging when the integrity of the system is compromised. In this case, the malicious agent could be a privileged insider.

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)

- For Financial Domains
  - What is the likelihood of reporting a corrupted payee in a financial transaction? (I)
  - What is the likelihood of reporting a corrupted payment amount in a financial transaction? (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 it takes to restore the data and/or service to its previous state. Just as before, restoral of 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 had not been not detected.

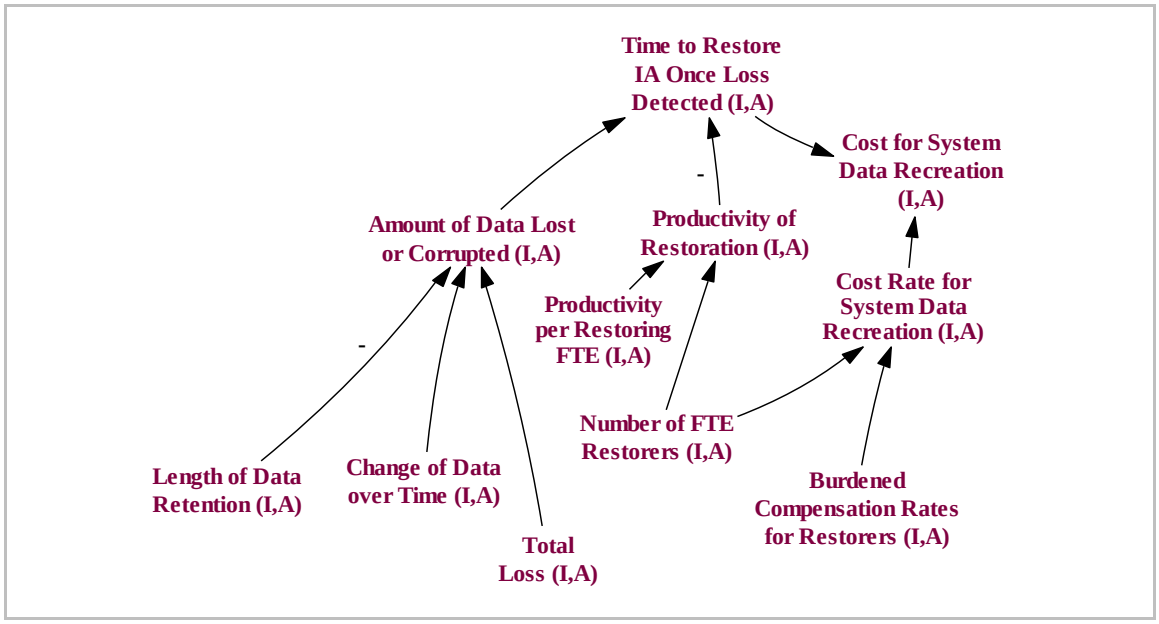


Figure 6: Time to Restore IA Once Loss Is Detected

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 system data re-creation also depends on the burdened compensation rates for 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 service/data once its inaccessibility is detected? (A)
  - How long does it take to restore 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 (FTE) 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 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 that depend on the service and/or data for their job performance. Lost revenue often occurs in systems that involve authorization or approvals since those may 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.

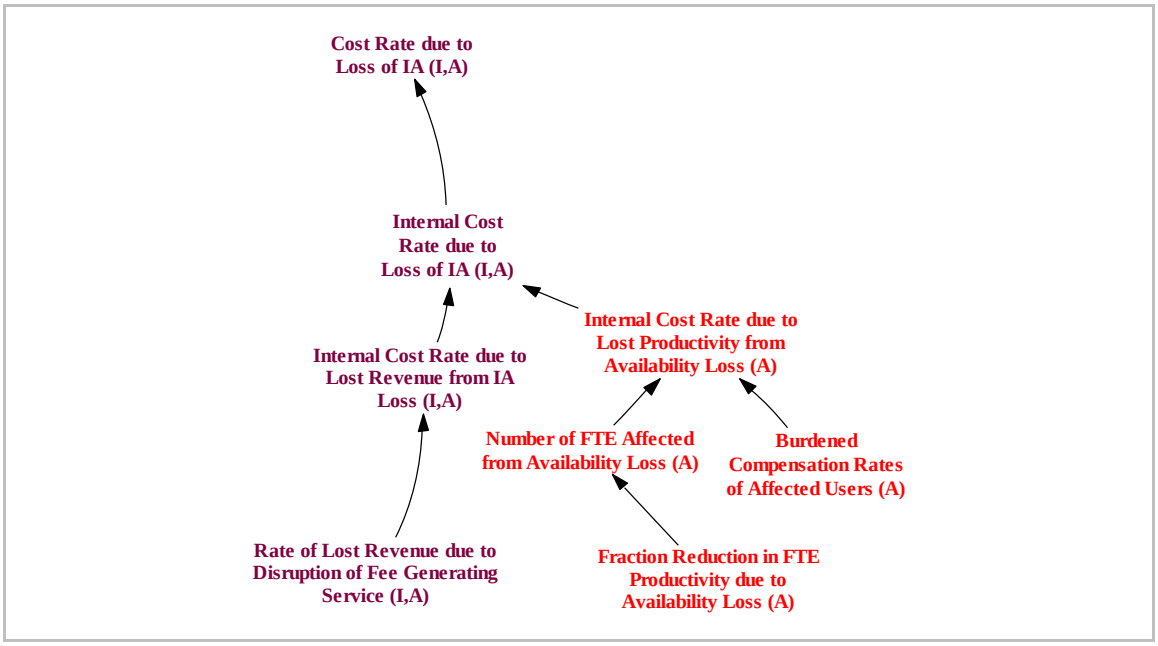


Figure 7: Internal Cost Rate due to Loss of IA

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 service/data? (A)
  - What is the percentage reduction of productivity due to inaccessible service/data? (A)
  - What is the burdened compensation rate of affected users? (A)

6.2 External Cost Rate Due to 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, including a potential increase 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; these costs are not further elaborated here.
- **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 amplified 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 disruption of payouts.

- **Safety**. The human safety domain calculates cost based on 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.[9] Other allowable costs for injury include costs of lost productivity since the injured party recovers full function, and any disability claims that result from complete loss of ability to function at work.

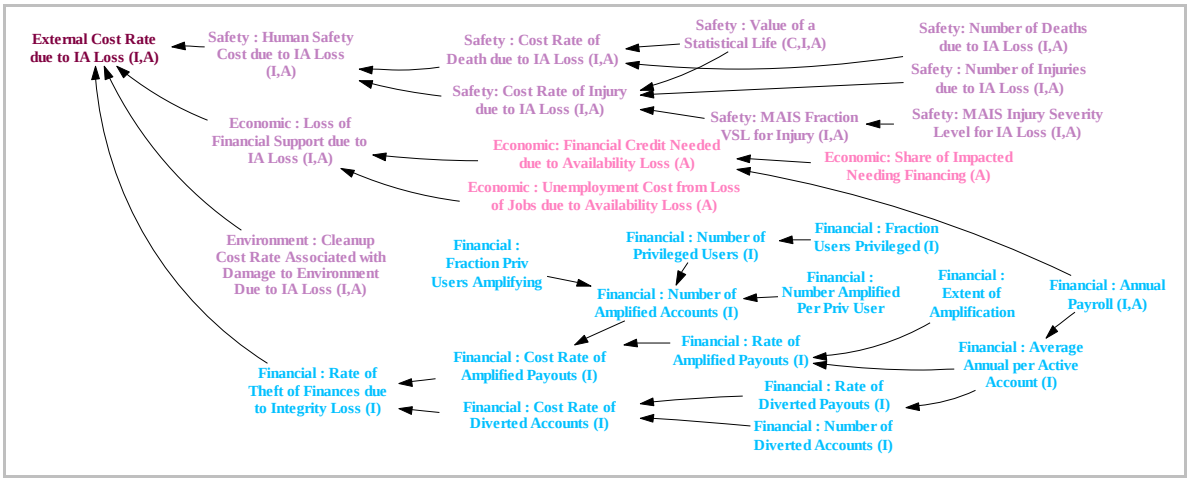


Figure 8: External Cost Rate due to IA Loss

Relevant questions to this portion of the factor tree include the following:

For the Safety View

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

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

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 amplification of a payout is possible without triggering additional checking or alerting? (I)

6.3 Cost Due to Loss of Confidentiality

As shown in Figure 9, costs of 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 credit monitoring costs of victims. Victim response costs to the organization depend on the number of individuals impacted[10] and the type of individual information lost. Historically, costs due to loss of Protected Health Information (PHI) are greater than loss of PII, so these will likely require different considerations for loss magnitude estimates.[11]

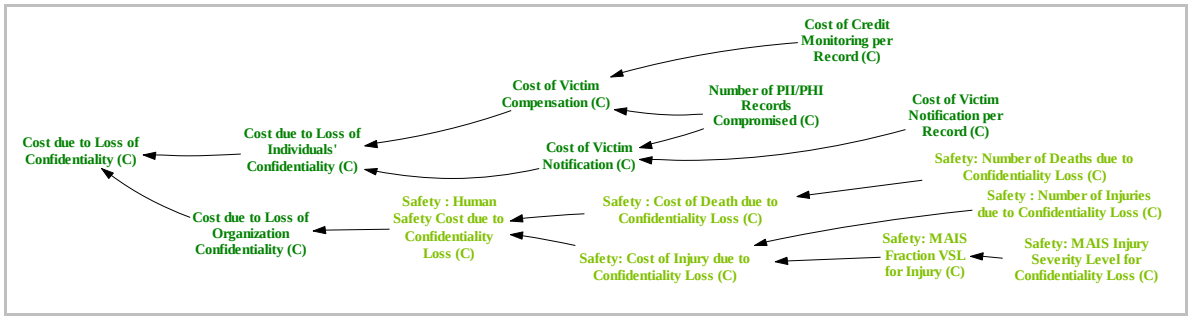


Figure 9: Cost Due to Loss of Confidentiality

While costs due to the disclosure of other sensitive organizational information is difficult to quantify in general, for the human safety domain, disclosures could compromise the identity of government personnel, even undercover agents, and result in 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 records are at risk of unauthorized disclosure? (C)
- How many individuals' PHI records are at risk of unauthorized disclosure? (C)

---

[10] 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. (2020). *2020 Information Risk Insights Study*. https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf

[11] Coburn, et.al. (2019). *Solving Cyber Risk: Protecting Your Company and Society*. Wiley, pg. 39.

- What is the cost of victim notification per number of victims notified? (C)

For the Safety View

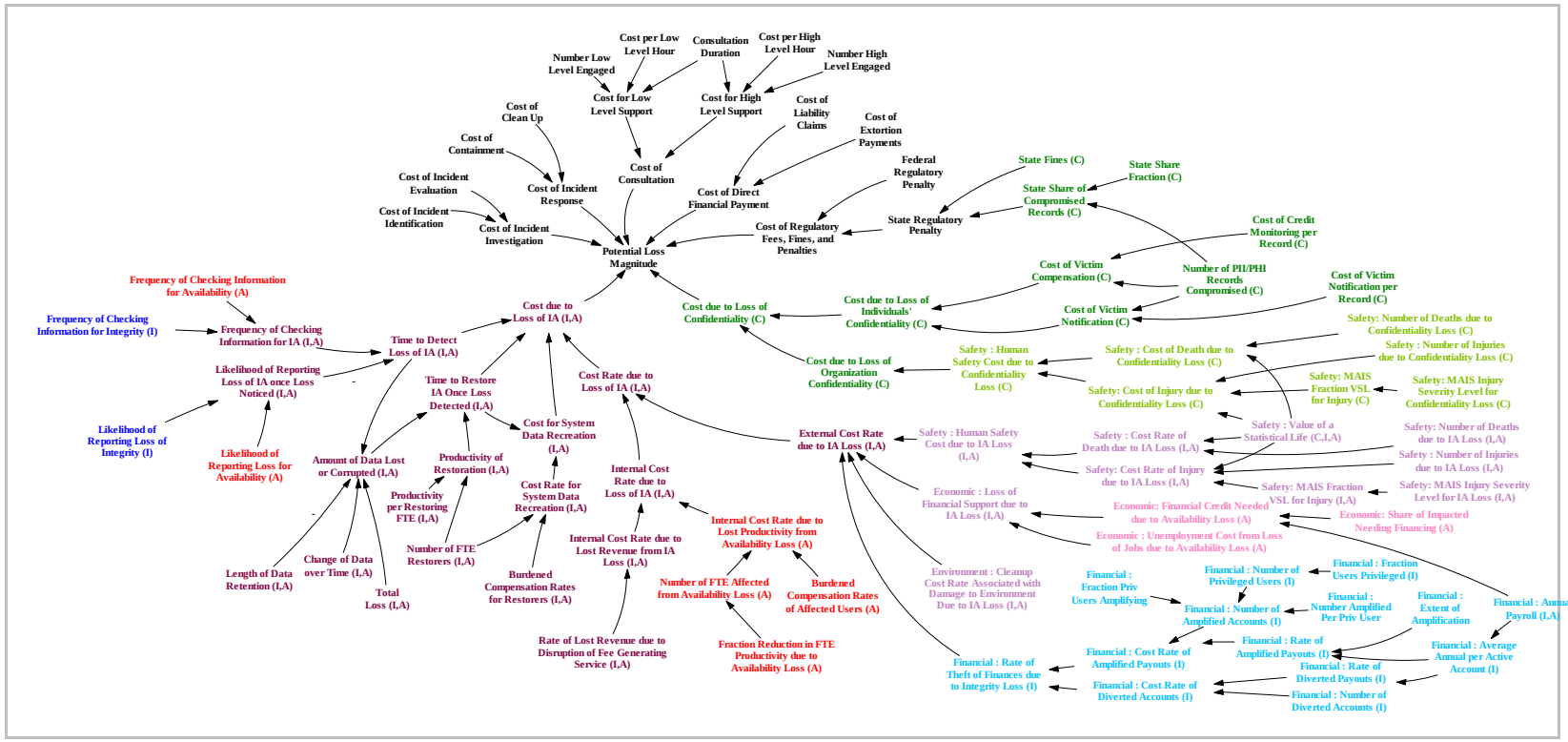
- How many deaths will result due to loss of confidentiality? (C)
- How many injuries will result due to loss of confidentiality? (C)
- What is the severity of injuries that result due to loss of confidentiality? (C)

7 Conclusion

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

We recommend additional research to refine and update factor tree inputs to the executable model as new or additional information becomes available and extend its use for risk mitigation decision support. Part of this research could include developing an extended review of factors noted as relevant to losses in recent cyber loss reporting. As part of the research we also recommend conducting sensitivity analysis on the various factors to understand which are key to the highest potential losses and which have potential for extensive growth. Additionally, a separate review of SAR assessments and their responses would help determine which types of systems are under-represented in the assessment history.

Appendix: Potential Loss Magnitude Factor Tree



Notation:

- F1 → F2 : Direct Relationship: Increasing Factor 1 tends to increase Factor 2; decreasing Factor 1 tends to decrease Factor 2.
- F1 → F2 : Inverse Relationship: Increasing Factor 1 tends to decrease Factor 2; decreasing Factor 1 tends to increase Factor 2.
- Black Type : Associated with All Three Loss Categories C, I, and A
- Dark Purple Type : Associated with Two Categories and Generally Applicable
- Light Purple Type : Associated with Multiple Categories but Specific to a System Loss View
- Dark Green Type (C) : Restricted to Confidentiaity and Generally Applicable
- Light Green Type (C) : Restricted to Confientiality but Specific to a System Loss View
- Dark Blue Type (I) : Restricted to Integrity and Generally Applicable
- Light Blue Type (I) : Restricted to Integrity but Specific to a System Loss View
- Dark Red Type (A) : Restricted to Availability and Generally Applicable
- Light Red Type (A) : Restricted to Availability but Specific to a System Loss View