DRDC | RDDC
technologysciencetechnologie

Preliminary Research Investigation Report: Remediation Cost Factors List

Delfin Y. Montuno
Solana Networks

Prepared by:
Solana Networks
301 Moodie Drive
Suite 215 Nepean, ON K2H 9C4
Canada

PSPC Contract Number: W7714-115274
Technical Authority: Maxwell Dondo, DRDC – Ottawa Research Centre
Contractor's date of publication: September 2018

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2019-C029
February 2019

Canada

IMPORTANT INFORMATIVE STATEMENTS

Preliminary Research Investigation Report

Remediation Cost Factors List

Version 1.0
26 September 2018

SOLANA
NETWORKS

List of Authors

Delfin Y. Montuno **delfin.montuno@solananetworks.com**

Abstract

Remediation activities occupy a significant amount of time for network defenders. In order to effectively manage those activities, network defenders need tools and methodologies to assist them. One approach that could help network defenders in that effort is to assign cost measures to remediation activities. Determining such a cost measure is not trivial, and researchers have suggested methodologies which require knowledge of the factors that influence the cost of remediation. Unfortunately, there is no exhaustive list of such cost factors. Through a task by Defence Research and Development Canada (DRDC)'s Cyber Decision Making and Response (CDMR) project, this report documents our research efforts in determining an exhaustive list of factors that could influence remediation costs. Our sources of information are publicly available literature as well as our experiential knowledge in cyber security. We further suggest techniques that could be used to aggregate the cost factors into cost measures that could be used by defenders in prioritizing network defence activities. We further propose ways of validating those proposed measures. As recommendations for next steps, we suggest further research be carried out on algorithms that contextually aggregate relevant factors to provide dynamic and missions-relevant cost measures, which are important for applications within the Canadian Armed Forces (CAF).

Résumé

Les défenseurs du réseau ont besoin d'outils et de méthodes favorisant une gestion efficace des travaux d'assainissement pour lesquels ils consacrent beaucoup de leur temps. L'attribution de mesures économiques aux travaux d'assainissement est une approche pouvant les aider à cet égard. La détermination d'une telle mesure des coûts n'est pas banale et les méthodes suggérées par les chercheurs exigent une connaissance des facteurs qui influent sur le coût de l'assainissement. Malheureusement, il n'existe pas de liste exhaustive de ces facteurs. Dans le cadre d'une tâche du projet de Prise de décision et intervention en cybernétique (PDIC) de Recherche et développement pour la défense Canada (RDDC), ce rapport précise nos efforts de recherche pour dresser une liste exhaustive des facteurs qui pourraient influencer les coûts d'assainissement. Des documents accessibles au public, ainsi que nos connaissances expérientielles en matière de cybersécurité ont servi de sources d'information. En outre, nous suggérons des techniques de regroupement des facteurs de coûts en mesure de coûts pouvant être utilisées par les défenseurs lors de la hiérarchisation des activités de défense des réseaux. Nous proposons également des moyens de valider les mesures envisagées. Pour les prochaines étapes, nous recommandons d'effectuer davantage de recherches sur les algorithmes regroupant les facteurs pertinents sur le plan contextuel pour fournir des mesures de coûts dynamiques et liées aux missions qui sont importantes au sein des Forces armées canadiennes (FAC).

Table of Contents

List of Tables

List of Figures

1. Introduction

This section provides the background and objective of this report. The objective, provided in Section 1.2, also outlines the contents of the remaining sections of this report.

1.1 BACKGROUND

Under the Defence Research and Development Canada (DRDC)'s Cyber Decision Making and Response (CDMR) project, the Automated Computer Network Defence (ARMOUR) project is being developed and executed as an integration framework with an end-to-end demonstration capability across the full Observe, Orient, Decide, Act (OODA) loop in the cyber domain. A detailed description of the defence integration framework is presented in [Nakhla-2017].

"ARMOUR uses the concepts of recommended remediation, CoAs (Course of Actions) and activities to support the decision-making process. Remediation costs and budget are utilized as part of the COADS (Course of Action Decision Support) computations. COADS uses the cost values to compute the optimal set of nodes to remove within a specified budget. The remediation costs could represent the amalgamation of many factors, such as financial resources, manpower, and time required to make the changes on the network, as well as operational impact." [Nakhla-2017].

Thus, there is not only the need to list all relevant cost factors associated with remediation actions but also to categorize their contribution meaningfully. This will allow us to aggregate them and to use them meaningfully in any of the remediation modes such as proactive, reactive, recovery, and non-remediation. This could help in determining a remediation cost measure that could be useful for CoA selection and prioritization similar to what was originally envisioned in ARMOUR [Sawilla-Burrell-2009].

1.2 OBJECTIVE

The objective of this report is to provide a list of cost factors that could contribute to a robust quantitative measure that is objective and repeatable and can be used by automated network defence capabilities such as ARMOUR [GD-CONOPS-2014, GD-ARMOUR-TD-2015]. Such a remediation cost measure could be leveraged in the computation and prioritization of network-level courses of action (COAs) in ARMOUR and other decision-support systems.

Specifically, this report addresses the requirements of Task TA 004 SOW (Remediation Factors to Support Determination of Remediation Cost Measure). The main areas of focus in this task are summarized below:

a) Review relevant literature on the definition of remediation cost to extract applicable cost factors [Task TA 004, Section 2.4.2]

b) Compile a list of cost factors and rationale of remediation cost that could be used by ARMOUR to determine a cost measure [Task TA 004, Section 2.4.3, Item 1]

c) Highlight and/or suggest any defence specific cost factors and their rationale [Task TA 004, Section 2.4.3, Item 2]

d) Suggest mathematical models that could be used to aggregate the cost factors into a cost metric [Task TA 004, Section 2.4.3, Item 3]

e) Provide ways to validate aggregation methodology suggested in d) above [Task TA 004, Section 2.4.3, Item 4]

f) Identify future investigation with respect to remediation cost measures [Task TA 004, Section 2.4.4]

A brief outline for each section of the report that addresses the above is given next.

Section 2 compiles a literature survey on how the cost of remediation actions is defined and used by the following network technologies that we identified in our research efforts: hardening solutions, intrusion detection solutions, network security investment solutions, and risk assessment solutions.

Section 3 presents lists of remediation cost factors extracted from the surveyed literature. The cost factors are described in the deployment, impact, and risk consequence categories that we determined to be relevant in this study. We further categorize the list of remediation cost factors in terms of remediation modes, actions, and their associated consequences as presented in Section 4.

In Section 5, we revisit the remediation cost based on the categorizations made in Section 4. The list of cost factors in this section was used for consultation with a subject matter expert (SME) in incident management to determine their defence relevance. To illustrate the ideas described in this section, we provide a hypothetical service impact cost example in Appendix A, which is listed as part of Section 10.

After reviewing Section 5 (except Section 5.5 which was added later) the SME noted that the proposed method of cost attribution “has yet to be witnessed in the enterprise” and thus the associated real data may not be readily available [Sarlis-2018]. He also suggested that conducting further study and leveraging the Common Vulnerability Scoring System (CVSS) could further refine the cost factors. He is of the opinion that automation be leveraged to mitigate the complexity of the cost factors computation. Incorporating war-time or peace-time context to the value of assets mentioned in Annex-1 of [Sarlis-2018] is addressed by the appropriate weights in the example given in Appendix A. Since remediation cost can be due to many cost factors which may not be readily apparent, a framework is provided in Section 5.5 to explain the significance of the different cost factors.

In Section 6, we suggest methodologies for aggregating cost factors[1]. Using a tree structure, we illustrate the inter-relationship of cost factors of different abstraction levels. The high-level aggregated cost factors needed for determining proactive and remediation sets are all expressed in monetary units. Section 6.5 lists the pros and cons of the proposed aggregation.

In Section 7, we suggest three validation methods for evaluating the reasonableness of the cost factors list and the results of applying the cost factors aggregation methods. In Section 8, we conclude this report with a list of recommendations on how to use the proposed cost factors tree, a list of future work, and a summary.

Following the references in Section 9, we provide the following supplementary research results in the appendices:

- A hypothetical service impact cost example (See Section 10.)
- Templates for organizing the cost factors of a remediation action for one or more missions (See Section 11) and for facilitating automating cost factors collection and computation
- Some weight setting formulas (See Section 12.) for use in the cost aggregation process
- Sample usage of the cost factors tree (See Section 13.)

Note that the following references were consulted but not referred to elsewhere in this report: [Ismail-2018, Kaspersky Lab, Ponemon Institute LLC, Smith-2017, theamegroup].

---

[1] These methodologies were not tested, but are just suggestions (as requested by the Task) of techniques that could be used to aggregate the cost factors.

2. Literature Survey

This section presents the results of a literature survey investigating cyber security solutions that incorporate the concept of cost. We are primarily interested in how remediation cost is formulated and used in the cyber security solutions. The relevant cyber security solutions that were uncovered include attack graph usage, network hardening, intrusion detection, network security investment, and security risk assessment.

The survey results are organized into the following subsections:

- Section 2.1.1 surveys existing attack graph solutions with respect to cost model
- Section 2.1.2 surveys hardening solutions that focus on minimal cost
- Section 2.1.3 surveys hardening solutions that consider some form of remediation cost
- Section 2.1.4 surveys hardening and intrusion detection solutions that consider cost of service impact
- Section 2.1.5 surveys mostly cost factors considered in intrusion detection solutions
- Section 2.1.6 surveys cost factors considered in network security investment and
- Section 2.1.7 surveys cost factors considered in risk assessment

2.1.1 Existing Attack Graph Solutions

This section surveys existing attack graph research by Cauldron, MulVAL, and NetSPA, SANS Institute, and others with respect to their remediation cost consideration.

2.1.1.1 Cauldron [Albanese-2012, Noel-2003, Noel-2009, and Wang-2006]

Albanese [Albanese-2012] considers a cost model in the selection of allowable actions. The model considers the impact of hardening actions that are interdependent. The hardening cost function is presented as “

> any function $cost : S \rightarrow R_+$ that satisfies the following axioms:
>
> $$cost(\emptyset) = 0 \quad (1)$$
>
> $$(\forall S_1, S_2 \in S)\ (C(S_1) \subseteq C(S_2) \Rightarrow cost(S_1) \leq cost(S_2)) \quad (2)$$
>
> $$(\forall S_1, S_2 \in S)\ (cost(S_1 \cup S_2) \leq cost(S_1) + cost(S_2)) \quad (3)$$

“

where S denotes the set of all possible strategies and $C(S)$ denotes the set of all the conditions disabled under strategy S.

The cost function produces values that can be used for comparisons and preserves size monotonicity. A simple cost function suggested is the cost value being equaled to the cardinality of $C(S)$. Otherwise, there is no further elaboration of the cost function.

Jajodia [Jajodia-2011] describes Cauldron, which has advanced capabilities for mission-centric cyber situational awareness but does not discuss any cost factor consideration.

Noel [Noel-2003, Noel-2009] has an implicit cost model in which the network administrator is assumed to have assigned relative costs for individual hardening measures. Their minimum-cost hardening solution selects the configuration with the lowest total cost. The authors briefly describe the computation of the overall cost of a particular hardening assignment being the sum of the individual hardening measures, assuming the costs are independent.

2.1.1.2 DRDC [Sawilla-Burrell-2009, Sawilla-Burell-2010]

Sawilla and Burrell [Sawilla-Burrell-2009, Sawilla-Burrel-2010] consider the following cost factors in the selection of remediation actions:

- patch availability
- resource costs
- usability: disruption of network function and impairment to organization business activity
- remediation cost
- financial cost
- time investment cost

Although the above cost factors are mentioned, the authors use weight in generic cost units to represent the cost in terms of time, money, and usability associated with a remediation action. Mapping of the cost factors to the weight is not explicitly discussed.

2.1.1.3 MulVal [Ou-2005, Homer-2009]

Ou [Ou-2005] presents a logic-based network security analyzer without explicit discussion or consideration of cost. The authors make certain assumptions and leave the cost problem as an open question.

Homer [Homer-2009] presents a security management solution based on Boolean Satisfiability Solving (SAT Solving) to find a mitigation solution. Their solution minimizes cost that arises due to security risk and usability impairment. The authors assume cost values are already available without going into any detail of how to obtain them.

2.1.1.4 NetSPA [Ingols-2009, Lippmann-2006]

Ingols [Ingols-2009] presents enhancements to NetSPA including (i) modeling of present-day threats and countermeasures (ii) point-to-point reachability algorithm, and (iii) a data structure to support reverse reachability. The paper does not explicitly consider the cost factors of countermeasures.

Lippmann [Lippmann-2006] presents the NetSPA solution which analyzes firewall rules and vulnerabilities to construct attack graphs. NetSPA produces a small set of prioritized recommendations without considering explicitly the cost factors of the recommendations.

2.1.1.5 SANS Institute [Vandeberghe-2007]

Vandengerghe [Vandenberghe-2007] describes the service impact of course of action in response to a computer network incursion. Determining which services or devices are affected is based on network fragmentation due to the course of action taken. The service impact is equal to the total value of services and devices affected. The author suggests that the value of service or device may be assigned a value between 1 and 10, the magnitude being a measure of its overall impact on the mission or event.

2.1.1.6 Others [Boddy-2005 Jha-2002]

Other related research results include the following.

Boddy [Boddy-2005] considers generation of adversary courses of action without considering explicitly cost factors of the action.

Jha [Jha-2002] claims to present a technique that performs simple cost-benefit trade-off based on the likelihoods of attacks. However, the cost measure is not explicitly discussed. We infer that the cost measure in this paper may be based on the number of atomic attacks.

2.1.2 Minimal-Cost Solutions

This section surveys remediation solutions that seek to minimize the hardening cost.

Work by Albanese [Albanese-2012] has already been described in Section 2.1.1.1.

Bhattacharya [Bhattacharya-2011] uses an exploit dependency graph that has associated additive cost for executing individual exploits. The cost is used to find the minimum cost to exploit the network vulnerabilities and not to find the minimum cost to remediate the vulnerabilities.

Chen [Chen-2008] defines a minimum cost network hardening solution as the minimum set of conditions that need to be removed to guarantee that no attack path remains and, at the same time, the total cost of the set of conditions is minimal. However, the authors assume rectifying each condition has an associated cost without providing any guidance on how to quantify it.

Work by Homer [Homer-2009] has already been described in Section 2.1.1.3.

Idika [Idika-2009] presents a solution that considers limited budget in choosing security measures which have associated cost. Their model assumes, however, "that the network administrator is able to assign costs to the hardening measures in terms of money or time."

Islam [Islam-2008] proposes a heuristic algorithm to compute the total cost of initial conditions that need to be disabled. They assume the cost of disabling each initial security condition is available. Some of the cost factors mentioned are the monetary cost of upgrading hardware or software and the administrative costs in time.

Work by Noel [Noel-2003, Noel-2009] has already been described in Section 2.1.1.1.

Saha [Saha-2016] quantifies inherent vulnerabilities and hardening cost for the system being protected. However, the hardening cost is described in terms of the number of leaves that need to be secured. The question of cost assignment with a meaningful value is not discussed.

Wang [Wang-2006] proposes a solution that considers multi-step intrusion in hardening a network. However, the hardening cost is described in terms of the number of initial conditions that are expressed in disjunctive normal form (DNF), and is not described in terms of the assigned cost value to the initial conditions. The authors assume the existence of a cost model with at least a partial ordering property.

Wang [Wang-2008] mentions various factors listed below that may affect the hardening actions:

- environmental factors - this includes latency in the availability of software patches or hardware upgrades
- cost factors - this includes budget and administrative effort required for deploying patches and upgrades
- mission factors - this includes organizational preferences for service availability and usability over service security

The paper does not examine the above listed factors in any further detail beyond the cursory listing as mentioned above.

Wang [Wang-2013] proposes a middleware solution that uses a Hidden Markov Model (HMM) to explore vulnerability information represented in an attack graph. Although the solution allows specification of cost factors, the authors do not discuss how to quantify those factors. The authors list the following two cost metrics:

- attack cost which is the result of one or more of the following:
    - confidentiality loss
    - integrity loss
    - denial of service
    - public embarrassment
    - privilege escalation
- defense cost which is the result of one or more of the following:
    - system downtime
    - installation cost
    - operation cost
    - training cost
    - patch incompatibility cost

2.1.3 Remediation Cost Factors

This section surveys remediation solutions that include some discussion of cost factors.

Butler [Butler-2002] proposes a multi-attribute risk assessment approach which security specialists can use to estimate the benefit of countermeasures in reducing organizational risk. The paper presents a cursory mention of cost factors such as purchase, implementation, operational, and maintenance costs.

Dewri [Dewri-2007] develops a model to quantify the potential damage in a system described by the corresponding attack tree and also quantifies the cost of the security hardening measures. The five different cost components identified are – installation (monetary), operation cost (monetary), system down-time (time), incompatibility cost (scale), and training cost (monetary). The paper does not indicate how the factors are to be converted to the same unit so that they can be combined meaningfully together into a single cost. In addition the paper does not clarify how "incompatibility" costs are determined.

Kijsanayothin [Kijsanayothin-2010] provides a solution to assist security administrators in choosing the most cost-effective set of countermeasures to remediate security flaws found in an attack graph. The three decision variables used are:

- $countermeasure$ set which is the minimal set of countermeasures for a set of security flaws
- $cost$ which has three categories, $\{low, medium, high\}$ that could have a range of values
- *effort* which has two categories, $\{week, month\}$

Pendleton [Pendleton-2016] surveys system security metrics in the following areas:

- system vulnerabilities
- defense power
- attack or threat severity
- situations

The authors define cost metric as "the amount of resources consumed including deployment, operating, and maintenance cost". No further elaboration of the cost metric is given.

2.1.4 Operational Impact Cost Factors

This section surveys remediation solutions that consider operational impact cost factors.

Kheir [Kheir-2009] describes how to evaluate the effect of security incidents on offered services. Their service dependency graph defines how the security related properties of one part of the graph affects another. The security properties considered are confidentiality (C), integrity (I), and availability (A).

Kheir [Kheir-2010] bridges the gap between network vulnerability models that describe how vulnerabilities could be exploited and service dependency models that describe how services affect each other. The authors claim that their proposed service dependency representation can be used to evaluate intrusion and response cost. The cost model is based on Return on Response Investment $RORI = \frac{RG-(CD+OC)}{CD+OC}$, where

- RG is response goodness
- CD is collateral damage (side effect of the response)
- OC is operational costs (It includes response setup and deployment costs, such as manpower and over provisioning.)

Kotenko [Kotenko-2012] proposes combining attack graphs and service dependency graphs to allow for calculation of security metrics and associated cost. However, the authors did not describe how costs are to be assigned.

Work by Vandenberghe [Vandenberghe-2007] has already been described in Section 2.1.1.5.

2.1.5 Cost Factors in Intrusion Detection Solutions

This section surveys intrusion detection solutions that consider cost factors.

Gaffney [Gaffney-2001] describes cost in the intrusion detection context which involves the cost of making the right decision. However, methodologies to quantify it are not given.

Kumar [Kumar-2016] describes cost factors in the intrusion detection context. The factors include:

- damage cost: damage caused by hackers
- response cost: cost of the reactive action taken
- operational cost: cost of processing and analyzing intrusion events
- detection cost: cost due to false negative alarms, false positive alarms, true positive alarms, and true negative alarms

The paper does not clarify the means of quantifying the above cost.

Lee [Lee-2002] describes cost factors in the intrusion detection context in a similar manner to [Kumar-2016]. The major cost factors involve development costs, operational costs, damage costs, and costs in the response.

Stritapan [Stritapan-2011] provides a metrics framework for computer security incident response (CSIR) that includes the following components:

- cost which includes
    - cost to maintain incident response (IR) capabilities
    - cost to remediate an incident
    - cost to implement a change in an IR program
    - intangible cost consisting of but not limited to reputation and trust
    - cost due to labor, material, and overhead
- time - total time it takes to resolve an incident
- quality - how well an incident is resolved

Stakhanova [Stakhanova-2012] provides a solution for responding cost-sensitively to intrusion. The cost includes the following:

- potential costs associated with the intrusion handling process
    - mandatory reporting requirements
    - cost of intrusion detection equipment
- response cost consisting of the following two factors
    - negative effect of a response on the system
    - operational cost of the action associated with the response maintenance

Stolfo [Stolfo-2000] describes a cost-based modeling approach for intrusion detection. The author takes a cost accounting model used for fraud detection and applies it to intrusion detection. The cost factors of their cost-based models for intrusion are very similar to those discussed in [Kumar-2016] and [Lee-2002]. The factors include damage cost, challenge (response) cost, and operation cost.

Strasburg [Strasburg-2009b] proposes a methodology to assess intrusion response cost. Their cost factors are

- response operational cost due to constant maintenance of the response
- response goodness cost that measures how well the intrusion is contained
- response impact cost that measures the response effect on the system functionality

The paper includes detailed discussion of the above factors, providing perspective that may be useful as we carry out more detailed research into remediation cost factors.

Wei [Wei-2001] describes a cost model for network intrusion detection systems based on their investigation of the cost factors of assets and categories of various intrusions.

2.1.6 Cost Factors in Network Security

This section surveys research work on cost factors in the provision of network security in general.

Bistarelli [Bistarelli-2006] presents an approach for evaluating Information Technology security investments based on the defender's return on security investment and the attacker's return on attack. Some of the cost factors are:

- asset value - consists of the cost of creation, development, support, replacement, and ownership values of an asset
- financial loss - a function of a single loss exposure and the annualized rate of occurrence
- return on investment - a function of financial loss and the cost of security investment

Chen [Chen-2004] describes the architectural and policy recommendation costs in the context of asset management. Appendices K and L in the paper provide examples of the respective cost components.

Cremonini [Cremonini-2005] evaluates security investment from the perspective of an attacker's return on attack. The cost model may include both tangible and intangible losses such as costs for data recovery and damage to reputation, respectively. No details are provided about the method for quantifying the costs.

An ENISA report [ENISA-2012] describes the need to measure the Return on Security Investment (ROSI). The various factors considered in the measure such as actual cost of an incident may be useful for our cost factors consideration.

Gordon [Gordon-2002] presents a framework for evaluating security investment decisions. The loss model considered depends on threat probability, information set vulnerability, and monetary loss. Monetary loss is caused by security breach on the information set that relates to confidentiality, integrity and denial of services.

Keramati [Keramati-2011] computes the effective cost of vulnerability and initial condition based on the actual cost assigned by network administrator and the rate of occurrence of the said condition on the attack scenario.

Keramati [Keramati-2012] proposes a security metric that is a function of network confidentiality, integrity, and availability for attack graph to quantitatively measure the security risk of possible attacks. Cost factors mentioned are similar to those described in [Wang-2008].

Mercuri [Mercuri-2003] analyses security costs in general without going into the details of cost factors.

Noel [Noel-2010] extends risk analysis to include associated network operational costs, attack impact costs and others. The analysis is used to quantify whether additional security investment is justifiable based on the expected losses arising from security breaches. Although specific examples such as the cost of recovering from a database breach and implementing firewall changes are given, there are no recommendations on how to estimate the associated cost.

Pamula [Pamula-2006] considers the minimal sets of initial weakest adversary attributes needed to successfully compromise a network without explicitly involving any cost measure.

Poolsappasit [Poolsappasit-2012] develops a model to quantify the expected return on investment based on a user specified cost model and the likelihood of the system being compromised. The authors do not assume any particular cost model for both control cost and loss/gain evaluation. They indicate that any cost model is usually subjective to organizational policies.

2.1.7 Cost Factors in Risk Assessment

This section surveys work carried out to study the use of cost factors in the area of risk assessment.

Lala [Lala-2001] does not explicitly discuss cost factors but considers how to accelerate damage appraisal for speedy and accurate database recovery. Their findings could help reduce the cost of further information loss.

Grimaila [Grimaila-2007] stresses the importance of having a rigorous and well-documented, information asset-based risk management process to improve certainty and speed-up the impact assessment of an information incident.

Cherdantseva [Cherdantseva-2016] reviews cyber security risk assessment methods for SCADA systems. Some of this work has overlap with areas of interest for the remediation cost factors, including:

- calculating expected damage from a cyber threat
- assessing risk impact
- calculating total estimated revenue loss
- measuring operation risk using non-probability-based metrics

The Joint Task Force Transformation Initiative Interagency Working Group prepared a NIST report [NIST SP 800-30-2012] which provides a guideline for conducting risk assessments. Risk assessments are a fundamental component of an organization's risk management process. Key areas of interest which overlap those of the remediation cost factors are:

- identifying impact to organizations that may occur given the potential threats of exploiting vulnerabilities
- identifying the likelihood that harm will occur

3. List of Remediation Cost Factors

In listing the remediation cost factors, we make the following assumptions:

- a computer network exists to provide a set of services for a set of personnel or systems for one or more missions
- a set of courses of action is available for remedying a corresponding set of vulnerabilities
- the cost of a remediation action can be determined based on its cost factors if known

The four general types of remediation cost with their corresponding consideration of cost factors as compiled from the literature survey are:

- Implicit remediation cost
  - These cost factors are implicit in the mind of the person assigning the cost. Section 3.1 describes implicit cost in more details.
- Remediation deployment cost
  - Section 3.2 describes the cost factors associated with the cost of deploying a remediation.
- Remediation impact cost
  - Section 3.3 describes the cost factors associated with the impact cost of deploying a remediation
- Cost of no remediation action
  - Section 3.4 describes the cost factors associated with the cost of not deploying a remediation

3.1 IMPLICIT REMEDIATION COST FACTORS

In the case of implicit remediation cost factors, the cost factors are implicit in the mind of the person or organization assigning the cost. This mode of cost assignment is not very useful for identification of individual unique associated cost factors. However, qualitative consideration of cost assignment will help us understand some of the reasoning behind the cost factors. Essentially, a cost value is needed to determine a minimal-cost solution. It is thus reasonable to start with the number of initial conditions that have to be disabled and proceed to assign the cost of the corresponding remediation action. Different researchers use this mode of cost assignment in different ways - we summarize their work below and in Table 1.

Albanese uses the concept of disabling initial conditions, which he initially defined to simplify the cost metric [Albanese-2012]. As dependencies may exist among initial conditions, the authors proposed choosing the set of initial conditions that can be independently disabled. A very simple cost function can be computation of the cardinality of the set [Albanese-2012]. Further, instead of the set cardinality, the cost can be refined to account for the cost of removing each individual condition that is assigned by administrators [Albanese-2012].

Another approach is finding the smallest set of measures that keeps the network safe by removing the smallest set of atomic attacks [Jha-2002].

Chen [Chen-2008] considers the minimum cost network hardening solution as a subset of initial conditions whose removal ensures that the network is safe and the total cost is minimal. The cost is based on the cost of removing the initial conditions. However, they do not clarify how the cost is determined.

Noel [Noel-2009] assumes relative costs have been given for individual hardening measures before they describe their solution on an efficient minimum-cost network hardening via exploit dependency graphs.

Saha [Saha-2002]'s cost measure is a function of the cost of defending leaf nodes. However, they do not clarify how the cost is determined.

Wang [Wang-2006]'s cost measure is based on the cost of initial conditions. However, the cost of disabling each initial condition is delegated to the administrators.[2]

The remediation cost described in the following literature is based on some cost factors.

Kijsanayothin [Kijsanayothin-2010]'s cost measure is only a component of their decision making process. They use a Conditional Preference Net (CP Net) that graphically represents qualitative conditional preference relationships among decision variables. The decision variables are the effort in time units, cost in monetary scale, and set of countermeasures. The choice of countermeasures is then selected based on the effort and cost preference. Cost and

---

[2] Although, Wang [Wang-2006] did not mention how, we believe it is based on the administrators' knowledge and experience.

effort are not defined beyond the concept of unit and scale. However, they have characteristics of the cost factors involved in a remediation action.

Keramati [Keramati-2011] mentions the need to consider the cost and time aspect of hardening measures. Costs are assigned to initial conditions but they do not clarify how to determine the cost factors. The authors indicate the need to reduce the time to find a satisfactory solution.

Homer [Homer-2009] indicates that usability, the cost of deployment, and potential damage due to successful attacks should be factored into cost assignment. The authors suggest that cost assignment could be based on some cost policy such as minimum number of configuration changes and the number of compromised machines. The cost due to damage done could be dependent on where the damage would have occurred – a higher cost is assigned for a location deeper in the network.

Table 1 Implicit Remediation Cost

Cost Factors	Description	Rationale	Justification
Set of initial conditions disabled **[Albanese-2012], [Jha-2002], Chen-2008], [Saha-2016], [Wang-2006], [Kijsanayothin-2010], [Keramati-2011]**	Different COAs disable different sets of initial conditions	The smaller the set of initial conditions required to be disabled by a COA the more effective the COA is.	Cost of remediation action is related to the cardinality of the set of initial conditions
Cost policy based **[Homer-2009]**	Cost assigned due to policy such as equal cost or a cost representing network location affected.	Need to have a cost measure that reflects preference.	Need to be able to select solution based on cost.
Hardening measures **[Noel-2009]**	Assume that relative costs have been assigned for individual hardening measures	Relative cost is also a cost measure.	Relative cost may be sufficient.

3.2 REMEDIATION DEPLOYMENT COST FACTORS

In general, all remediation actions come with a cost. However, different researchers have proposed diverse set of definitive cost factors and their assignment. For example, Sawilla and Burrell [Sawilla-Burrell-2009] indicate the need to consider cost of patch availability, resource, financial, and time investment while others such as Stritapan [Stritapan-2011], Kumar [Kumar-2016], and Stakhanova [Stakhanova-2012] consider response cost.

We note that a specific remediation action may involve only some of the cost factors. Remediation deployment cost factors are described in more detail below and summarized in Table 2.

3.2.1 Patch Availability

A key approach to remediating vulnerabilities involves applying software patches to computing systems. If there is no patch available, then the cost of patching could be considered infinite[3]. In practice, a patch could either be freely available or may need to be custom coded. The need to consider patch availability is mentioned in [Sawilla-Burrell-2009], [Wang-2008], [Wang-2013], [Dewri-2007], and [Keramati-2012].

3.2.2 Patch Evaluation

If effort needs to be expended to determine the right patch for a vulnerability then this effort can be assigned a cost. Selection, testing, and even development work may be involved in evaluating the right patch to use. Sawilla and Burrell [Sawilla-Burrell-2009] consider unavailable patches as having infinite costs.

3.2.3 Remediation Effort

It takes personnel effort and time to administer a remediation. The need to consider this aspect is mentioned in [Sawilla-Burrell-2009] and [Kijsanayothin-2010]. Operational cost is mentioned in [Pendleton-2016], [Kheir-2010], and [Kumar-2016]. Labor and material are mentioned in [Stritapan-2011], Stakhanova-2012], [Stolfo-2000], [Strasburg-2009b], and [Noel-2010]. Though not further elaborated in the above literature, we can consider remediation effort in terms of personnel labor rate and the amount time spent.

3.2.4 Financial Cost

Financial cost refers generally to the cost of implementing a remediation [Sawilla-Burrell-2009]. Idika [Idika-2009] indicates that the network administrator assigns one in terms of money or time. Wang's [Wang-2008] cost factors include money and administrative efforts for deploying patches and upgrades. Other factors that might affect resolution of vulnerabilities are mission factors which are described in Sections 5 and 6.

Wang [Wang-2008] mentions that organizational preferences for availability and usability might have an associated financial cost. In [Keramati-2012], Keramati discusses the security metrics that tie cost spent and security improvement. Thus, financial cost is always a factor of

---

[3] This assumes that there are no workarounds. The infinite value represents a very large relative cost value that tells the remediation algorithms that fixing the problem is impossible.

a remediation action. We may be able to account for financial cost in part based on the other cost factors.

3.2.5 Invested Time

Time is needed to perform remediation. Invested time can therefore be accounted for in the cost factors [Sawilla-Burrell-2009,Idika-2009].

3.2.6 Installation Cost[4]

Both Wang [Wang-2013] and Dewri [Dewri-2007] discuss installation costs associated with the installation and configuration of security products. Installation costs may be more relevant in the case of a reactive remediation.

3.2.7 Training Cost

Both Wang [Wang-2013] and Dewri [Dewri-2007] discuss training costs. Training may be necessary for personnel to ensure proper remediation is carried out - unless the remediation process has been fully automated.

Table 2 Deployment Cost Factors

Cost Factors		Description	Rationale	Justification
Remediation cost[5] [Sawilla-Burrell-2009], (response cost [Stritapan-2011], Stakhanova-2012] [Kumar-2016], [Stolfo-2000])		The cost factors of deploying remediation consist of patch availability, resources used, financial cost, and invested time, installation, and training.	Remediation action is not free.	Resources are spent in the remediation process, therefore the associated cost needs to be accounted.
Patch availability [Sawilla-Burrell-2009], [Wang-2008], [Wang-2013], [Dewri-2007], [Keramati-2012]	Patch is available	The cost is the deployment cost of the patch.	Effort is needed in deploying the patch.	When a patch is needed, we need to consider its availability, deployment, testing, and compatibility.
	Patch needs to be developed or a workaround has to be found	The cost is associated with the development and the deployment of the patch or the time spend looking for workarounds.	Development and testing effort is needed to build a patch or effort is needed to look for workarounds.	
		On the other hand, the cost could be considered infinite if	No justifiable effort is available to find the right	

---

[4] Although Wang [Wang-2013] and Dewri [Dewri-2007] did not explicitly mention the installation of patches, we may also consider it to be included here.

[5] Each of the cost factors mentioned in this row is further expanded in the following rows of this table.

	a patch could not be found in time for the remediation	patch.	
Resource costs/Effort[6] **[Sawilla-Burrell-2009], [Kijsanayothin-2010], (Operational cost [Pendleton-2016], [Kheir-2010], [Kumar-2016]), (labor, material [Stritapan-2011], Stakhanova-2012], [Stolfo-2000], [Strasburg-2009b], Noel-2012])**	Resources and effort spent in the process of remediation	It takes resources and effort to deploy a remediation action.	The resources and effort spent is not free and may not be negligible.
Financial cost[7] **[Sawilla-Burrell-2009], [Idika-2009], [Wang-2008], [Keramati-2012]**	Money could be spent in the process of remediation	Money is needed to remediate.	Need to account for money spent.
Time investment cost[8] **[Sawilla-Burrell-2009], [Idika-2009]**	Cost due to amount of time invested	Time is needed to remediate.	Need to account for time spent.
Installation cost **[Wang-2013], [Dewri-2007]**	Installation of new hardware or hardware upgrade as part of the remediation process	Hardware costs money and so does the labor that goes with the installation.	Need to account for this expenditure.
Training cost **[Wang-2013], [Dewri-2007]**	Training of personnel	Training costs money.	Need to account for this expenditure.

---

[6] Resource costs and effort are cost factors that can be further decomposed as described in the first row of this table.

[7] Financial cost is yet another cost factors that can be further decomposed in term of time and personnel effort spent.

[8] Time is a basic cost factor that appears in many higher-level aggregated cost factors such patching cost and training cost.

3.3 REMEDIATION IMPACT COST FACTORS

Any change in a network has the potential to disrupt its function and thus, impair the organizational function that depends on the network. The need to consider this type of impact is mentioned in [Sawilla-Burrell-2009], [Wang-2008], [Vandeberghe-2007], [Wang-2013], [Dewri-2007], [Kheir-2010], [Strasburg-2009b], and [Keramati-2012]. This factor may be decomposed into service, device, and downtime factors. The cost factors are described in more detail in the following subsections and summarized in Table 3.

3.3.1 Service Impacted

Kheir [Kheir-2010] and Strasburg [Strasburg-2009b] indicate that the side effect of a response on system functionality has to be considered. Wang [Wang-2008] also indicates the need to account for service availability and usability. This side effect could be on the set of services impacted. Vandeberghe [Vandeberghe-2007] describes a means of enumerating affected services. What needs to be explored further is how to assign a value to each impacted service.

3.3.2 Device Impacted

Kheir [Kheir-2010] and Strasburg [Strasburg-2009b] indicate that the side effects of a response have to be considered. This side effect could be on the set of devices impacted. Vandeberghe [Vandeberghe-2007] describes a mean of enumerating affected devices. What needs to be explored further is how to assign a value to each impacted device.

3.3.3 System Downtime

The impact of a remediation could be on system downtime and must be accounted for as indicated in [Wang-2013] and [Dewri-2007]. Kheir [Kheir-2010] and Strasburg [Strasburg-2009b] indicate that the side effects of a response have to be considered. This side effect could be system downtime. A method is required to describe how system downtime can be quantified.

Table 3 Service Impact Cost Factors

Cost Factors	Description	Rationale	Justification
Usability/Operation **[Sawilla-Burrell-2009], [Wang-2008], [Vandeberghe-2007], [Wang-2013], [Dewri-2007], [Kheir-2010] (Collateral Damage), [Strasburg-2009b], [Keramati-2012]**	This is the disruption of network function and impairment to organization's business. The cost factor may be better accounted for by the other cost factors.	Remediation action may cause service disruption.	Need to account for service disruption.
Service impacted **[Vandeberghe-2007]**	A service that is being denied or slowed down	A remediation action may impact services.	Services being impacted have to be accounted for.
Device impacted **[Vandeberghe-2007]**	A device that is being disabled for use or disconnected for access	A remediation action may impact devices.	Devices being impacted have to be accounted for.
System downtime **[Wang-2013], [Dewri-2007], [Kheir-2010], [Strasburg-2009b]**	The time the system is not available for services/use.	Downtime occurs when services or devices are being impacted.	Cost of downtime to personnel productivity has to be accounted for.

3.4 NON-REMEDIATION RISK COST FACTORS

There is no cost when remediation action is not taken. However, the cost only occurs when a vulnerability that it is supposed to be mitigated has been exploited. Otherwise, it is just a risk. The cost to remediate a vulnerability that has been exploited will need to include those (proactive) cost factors listed in Sections 3.2 and 3.3. This is in addition to the various cost factors listed non-exhaustively in the following subsections and summarized in Table 4.

3.4.1 Confidentiality, Integrity, & Availability

The need to account for the loss due to confidentiality, integrity, and availability breach is mentioned by Kheir [Kheir-2009], Gordon [Gordon-2002], and Keramati [Keramati-2012].

3.4.2 Damage Cost

Damage could appear in many forms. Kumar [Kumar-2016] and Stolfo [Stolfo-2000] discuss damage cost and Noel [Noel-2010] discusses database related damage. Cremonini [Cremonini-2005] discusses the cost of data recovery. If the damage cost is in monetary form, it can be considered under financial loss.

3.4.3 Intangible Cost

Intangible cost takes many forms. Stritapan [Stritapan-2011] lists reputation and trust as two examples of intangible cost. Cremonini [Cremonini-2005] discusses reputation cost further.

3.4.4 Financial Loss

Financial loss could appear in many forms. Bistarelli [Bistarelli-2006] discusses loss that is a function of a single loss exposure and annualized rate of occurrence without providing more detail. Gordon [Gordon-2002] describes monetary loss as due to confidentiality, integrity, and availability – the former two relate to data while the latter relates to services.

Table 4 Cost Factors of No Remediation Action (doing nothing).

Cost Factors[1]	Description	Rationale	Justification
Confidentiality, Integrity, Availability [Kheir-2009], [Gordon-2002], [Keramati-2012]	Confidentiality and integrity of data, and availability of services/system	When vulnerability is exploited, CIA may be compromised.	Need to account for the loss due to CIA breach.
Damage cost [Kumar-2016], [Stolfo-2000], [Noel-2010], [Wei-2001], [Bistarelli-2006], [Cremonini-2005]	Damage could appear in various forms such loss of data and hardware/software assets.	Damages in whatever forms are costly.	Damages in whatever forms have to be accounted for.
Intangible cost (reputation and trust) [Stritapan-2011], [Cremonini-2005]	Reputation and trust that are promoted over time	It takes time and sometimes, money to develop good reputation and trust.	Loss of reputation and trust need to be accounted for.
Financial loss [Bistarelli-2006], [Gordon-2002]	Financial loss in terms of CIA breach or some other forms	Financial loss cannot be taken for granted.	Need to consider financial loss.

[1] The cost factors described here do not have the same level of abstraction and thus they are in some way interdependent. For example, loss of data integrity can incur damage cost and/or intangible cost depending on the specifics of the incident. If the incident is not known to the public, we may not have to consider the intangible cost due to loss of reputation. However, the loss of data integrity still can have a financial cost in term of the need for its recovery, if recovery is at all possible. Thus, only in the application to specific scenario could we (and we should) ensure independence and not double count cost.

4. Categorizing Remediation Cost Factors

To make the remediation cost factors described in Section 3 more amenable for their use in the COA selection process, we categorize them as follows:

- Remediation action and its associated consequences: The cost factors are further categorized as belonging to one of the following subcategories:
    - deployment cost
    - operation impact cost
    - risk cost
- Remediation modes: The cost factors are further categorized as belonging to one of the following subcategories:
    - proactive cost
    - reactive cost
    - non-action cost

Table 5 shows, with additional comments, the two dimensional view of the remediation cost factors on the basis of consequences and operational modes.

Table 5 Remediation Modes and Consequences Cost Factors

Conse-quences / **Modes**	**Deployment Cost**	**Operational Impact**	**Risk Impact**[1]	**Comments**
Proactive	Real	Real	Potential	Usually, risk impact is not a cost factor here.
Reactive	Real	Real	Real	The severity of its deployment cost and operational impact will be higher than that of the proactive mode. This mode overlaps in some way with the security incident handling.
Non-Action	Potential to real	Potential to real	Potential to real	Loss and impact cannot be completely ignored here. We need to consider the likelihood of the vulnerability associated with the remediation being exploited. Therefore, the cost and impact should be bounded by that of the reactive remediation mode.

[1] If loss occurs, the loss impact may linger over time – requiring long-term recovery effort.

After having described the cost factors associated with all the remediation modes, and the remediation action and its associated consequences, we make some observations on their availability, combination methodology, and confidentiality in Section 4.3.

4.1 COST FACTORS ACCORDING TO REMEDIATION CONSEQUENCES

This section describes the different factors which affect cost of remediating vulnerabilities. Categorizing these cost factors accordingly, we have the following categories:

- Deployment cost factors: Having to deploy a remediation action entails cost. See Section 4.1.1 for more details.
- Operational impact cost factors: Remediation causes changes which may impact the system being remediated. See Section 4.1.2 for more details.
- Risk cost factors: Loss occurs when a vulnerability which was not remediated in a timely fashion is exploited. See Section 4.1.3 for more details.

4.1.1 Deployment Cost Factors

Executing a remediation action requires effort and other resources. This deployment cost is due to the labor and time of the personnel involved and sometimes, the software and/or hardware used. For example, the effort of software patching often involves the following steps [Schmeider-2016]:

- Obtaining the patch from a trusted party and validating patch and source integrity
- Testing the patch to ensure the vulnerability is remediated and the patch will not break other applications – a lengthy and laborious process
- Notifying affected parties of the unscheduled downtime if needed
- Deploying the patch
- Testing for post-deployment operational efficiency
- Rollback and remediation, if needed
- Documenting the result of the patching effort

Some values listed above have to be estimated before patching and this is where historical data could be helpful. This also signifies the importance of good record keeping, from which useful estimates could be derived.

Therefore, the labour will vary depending on what needs to be done for different scenarios and the form of remediation action required. For example, if the patch for vulnerability is already available, then no additional cost for determining, testing, and even developing the right patch has to be considered. Nevertheless, we can account for the deployment cost factors as consisting of labor, time, software, hardware, training, and training time. The rationale, pros, and cons of these cost factors are presented in Table 6.

Table 6 Remediation Deployment Cost Factors

Factor	Rationale	Pros	Cons	Comments
Effort Cost Factors				
Labor	Need effort to deploy a remediation action.	Account for the required effort.	Need to estimate the effort and hourly rate needed for each remediation action in each scenario.	The estimates may be subjective but required to make the process accountable.
Time	Need time to deploy a remediation action. In general, labor requires time.	Account for the required time.	Need to estimate the required amount of time.	Same as above.
Material Cost Factors				
Software	May need new software and/or to modify existing software. Needed software may not be free.	Account for cost beyond effort.	Need to estimate software cost without double counting the above labor cost.	New software may not be needed or readily available
Hardware	May need new hardware and/or to modify existing hardware. Required hardware may not be free.	Account for cost beyond effort.	Need to estimate hardware cost without double counting the above labor cost.	New hardware may not be needed or readily available. This requirement may impact existing system setup.
Training Cost Factors				
Training	May need additional training.	Account for additional effort.	Need to estimate training cost without double counting the above labor cost.	Training may not be needed or readily available.
Time	Training takes time	Account for additional time.	Need to estimate training time without double counting the above labor time.	Do not to consider this time factor if training is not needed.

Table 7 provides an example of how the deployment cost could be computed.

Table 7 Proposed formulae for Computing Deployment Cost[5]

Cost	$subfactor_1$	sf_2	sf_3	sf_4	**Subtotal**
Cost of Accomplishing a Remediation Action					
Effort	$labor\_rate$	$time$	n_e[1]		$\sum_{i=1}^{n_e} labor\_rate(i) * time(i)$
Material	$software\_cost$	$hardware\_cost$	n_s[2]	n_h[3]	$\sum_{i=1}^{n_s} software\_cost(i) + \sum_{j=1}^{n_h} hardware\_cost(j)$
Training	$training\_rate$	$time_t$	n_t[4]		$\sum_{i=1}^{n_t} training\_rate(i) * time_t(i)$

[1] Number of effort instances

[2] Number of software

[3] Number of hardware

[4] Number of trainings

[5] Initially, the cost will have to be estimated by the Subject Matter Expert (SME) based on their knowledge and experience. Over time, if these estimates are recorded systematically with their corresponding rationale, they can be built on and more accurate estimates can be obtained.

4.1.2 Operational Impact Cost Factors[9]

Executing a remediation action results in changes to the system it is remedying. Until the process is successfully completed, it affects the normal operation of the system in a variety of ways. Services availability, devices accessibility, and information availability of the systems relied upon by users for achieving organizational objectives could be adversely affected. Table 8 describes the associated cost factors in more detail.

Table 8 Remediation Operational Impact Cost Factors

Factors	Rationale	Pros	Cons	Comments
Operational Availability Cost Factors				
Service	Services may be impacted by a remediation action.	Account for loss of services.	• Need to know the interrelationship of various services. • Need to understand the value of services in the overall organizational objective context. • Need to know which/how services are impacted	It is desirable to have the impacted services automatically enumerated.
Device	Devices hosting services may be impacted by a remediation action.	Account for impact on devices.	• Need to know which/how devices are impacted. • Need to know what services are hosted by which devices.	The value of a device may be a function, in part, of the services it is supporting.
Information	Information may not be accessible and/or available due a remediation action.	Account for loss of access and/or availability of information.	• Need to know which information set is affected. • Need to know who needs which information set	The value of information may depend on the user and the context of usage.
Personnel Cost Factors				
Labor	Labor is wasted when services and/or devices are impacted.	Account for loss in labor.	Need to know who are impacted and their corresponding labor rate.	This requires an accurate record of how the network is being used by whom.
Time	Time is wasted	Account for	Need to know who are	This requires an

---

[9] Initially, the cost will have to be estimated by the SME based on their knowledge and experience. Over time, if these estimates are systematically recorded with their corresponding rationale, it is possible to build on them and obtain more accurate estimates.

	when services and/or devices are impacted.	loss in time	impacted and their amount of wasted time.	estimate of period of device/service down time.

Table 9 provides an example of how to compute the operation impact cost.

Table 9 Suggested formulae for Computing Operational Impact Cost

Cost	$subfactor_1$	sf_2	sf_3	Subtotal
Operation[5]	$Value(s), where\ s\ \epsilon\ S$[1]	$Value(d), where\ d\ \epsilon\ D_s$[2]	$Value(i), where\ i\ \epsilon\ I$[3]	$\sum_{s\epsilon S}(Value(s) + \sum_{d\epsilon D_s} Value(d)) + \sum_{i\epsilon I} Value(i)$
Personnel	$labor\_rate_p$	$time_p$	n_p[4]	$\sum_{i=1}^{n_p} labor\_rate_p(i) * time_p(i)$

[1] Set of impacted services, S
[2] Set of impacted devices that are members of service $s\ \epsilon\ S$
[3] Set of impacted information, I
[4] Number of affected personnel
[5] Based in part on [Vandenberghe-2007]

4.1.3 Risk Cost Factors

Remediation actions are usually executed accurately. As a result, loss due to erroneous remediation actions is rare or considered negligible. In most cases, the risk materializes in the form of loss because the system being remediated is already breached. Thus, if we are considering non-remediation, we need to consider the situation where the risk actually does materialize and if so, what the loss would be. Table 10 lists the cost factors related to non-remediation action.

Table 10 Risk Cost Factors

Factors	Rationale	Pros	Cons	Comments
Reactive Loss Cost Factors				
Information	Information may not be accessible, available, and/or lost due a breach	Account for the loss of access and/or availability of information.	• Need to know which information set is affected. • Need to know who needs which information set	The value of information may depend on the user and the context of usage.
Reputation	Trust may be broken and reputation tarnished.	Account for the loss of reputation/trust due to a breach.	May be hard to quantify.	Loss here can be in the form of business-to-business, business-to-consumer relationship.
Monetary	Financial loss may result due to a breach.	Account for possible financial loss	May be hard to quantify.	Additional security insurance may be needed here to cover for the financial loss.
Compliance	Security non-compliant may have associated penalty.	Account for the penalty associated with security non-compliance.	May be hard to quantify.	Penalty may depend on the consequence of the loss due to a breach. Associating a remediation action and an exploit/breach may not be that direct.
Further	A breach may	Account for	May be hard to	Further analysis

Exploitation	facilitate subsequent exploits.	additional exploits.	quantify.	may be needed to determine the additional exploits, threats, and associated potential costs.
Mission goal/success/completion	A breach may compromise the completion and success of a mission.	Account for impaired success or failure to achieve expected goal.	May be hard to quantify.	May have to be evaluated on a case by case basis.

Proposed methods to quantify the different types of losses are described in Table 10. The approaches would need further investigation.

4.2 COST FACTORS ACCORDING TO REMEDIATION MODES

In Section 4.1, we describe different cost factors of a remediation action according to its associated consequences. To align the cost factors with the various decision making scenarios, we organize them here according to following remediation modes:

- Proactive remediation: A remediation action is taken before the targeted vulnerability has been exploited. See Section 4.2.1 for more details.
- Reactive remediation: A remediation action is taken after the targeted vulnerability has been exploited. See Section 4.2.2 for more details.
- No remediation action is taken: No remediation action is taken proactively for the targeted vulnerability - a vulnerability that has a non-zero probability of being exploited. See Section 4.2.3 for more details.

4.2.1 Proactive Remediation

When a vulnerability is proactively remediated, we only have cost factors of deployment cost from Table 6 and operational impact cost from Table 8. Combining the corresponding cost formulas from Table 7 and Table 9, we arrive at the formulas shown in Table 11 for computing the proactive remediation cost. To determine a monetary value for the “Operation” cost is a subject for further investigation, which is beyond the scope of this task. See Section 4.3 for some discussion on “Operation” cost.

Table 11 Proposed formulae for the cost of proactive remediation

Cost	$subfactor_1$	sf_2	sf_3	sf_4	Subtotal
Cost of Accomplishing a Remediation Action					
Effort	$labor\_rate$	$time$	n_e[1]		$\sum_{i=1}^{n_e} labor\_rate(i) * time(i)$
Material	$software\_cost$	$hardware\_cost$	n_s[2]	n_h[3]	$\sum_{i=1}^{n_s} software\_cost(i) + \sum_{j=1}^{n_h} hardware\_cost(j)$
Training	$training\_rate$	$time_t$	n_t[4]		$\sum_{i=1}^{n_t} training\_rate(i) * time_t(i)$
Operational Impact Cost of Accomplishing a Remediation Action					
Operation[9]	$Value(s), where$ $s \epsilon S$[5]	$Value(d), where$ $d \epsilon D_s$[6]	$Value(i),$ $where$ $i \epsilon I$[7]		$\sum_{s \epsilon S} (Value(s) + \sum_{d \epsilon D_s} Value(d)) + \sum_{i \epsilon I} Value(i)$
Personnel	$labor\_rate_p$	$time_p$	n_p[8]		$\sum_{i=1}^{n_p} labor\_rate_p(i) * time_p(i)$

[1] Number of effort instances
[2] Number of software
[3] Number of hardware
[4] Number of trainings
[5] Set of impacted services, S
[6] Set of impacted devices that are members of service $s \epsilon S$
[7] Set of impacted information, I
[8] Number of affected personnel
[9] Based in part on [Vandenberghe-2007]

4.2.2 Reactive Remediation

In the case where no proactive remediation action is taken and a subsequent reactive remediation action becomes necessary, then the cost factors will be as shown in Table 12.

Table 12 Cost of Reactive Remediation

Cost	$subfactor_1$	sf_2	sf_3	sf_4	Subtotal
Cost of a Breach Recovery Action					
Effort	$labor\_rate$	$time$	n_e[1]		$\sum_{i=1}^{n_e} labor\_rate(i) * time(i)$
Material	$software\_cost$	$hardware\_cost$	n_s[2]	n_h[3]	$\sum_{i=1}^{n_s} software\_cost(i) + \sum_{j=1}^{n_h} hardware\_cost(j)$
Training	$training\_rate$	$time_t$	n_t[4]		$\sum_{i=1}^{n_t} training\_rate(i) * time_t(i)$
Operational Impact Cost of a Breach Recovery Action					
Operation[9]	$Value(s), where$ $s \in S$[5]	$Value(d), where$ $d \in D_s$[6]	$Value(i),$ $where$ $i \in I$[7]		$\sum_{s \in S} (Value(s) + \sum_{d \in D_s} Value(d)) + \sum_{i \in I} Value(i)$
Personnel	$labor\_rate_p$	$time_p$	n_p[8]		$\sum_{i}^{n_p} labor\_rate_p(i) * time_p(i)$
Loss due to the Security Breach					
Information	$loss$				
Reputation	$trust$				
Monetary	$budget$				
Compliance	$penalty$				
Further Exploitation	$exploit$				

[1-9] See footnotes in Table 11.

Although, the factors shown in Table 12 have the same names as those shown in Table 11, their actual values may differ due the difference in context. In fact, their corresponding actual values will be substantially higher due to the breach that has occurred and may still be on-going. For example, the effort has to account for the extra cost of containing and recovering from the breach. Note it also has the additional cost factors associated to the loss due to the security breach.

As mentioned in Section 4.1.3, determining the risk cost factors is a subject requiring further investigation and thus we have no corresponding cost formulas for it.

4.2.3 Non-Remediation

In the case when no remediation action is taken and no subsequent remediation action is necessary, then the cost factors that are ignored are those illustrated in Table 12**Error! Reference source not found.**. Inaction has an associated risk. In Section 4.2.3.1, we discuss the conditions when the risk of inaction is unacceptable.

4.2.3.1 To Remediate or Not to Remediate

Although it may appear that taking no remediation action will cost nothing, we need to be mindful that ignored vulnerabilities can be exploited with dire consequences.[10] We describe next a means of deciding when ignoring the remediation action might be unacceptable.

Let us define first the following parameters:

- p: the probability, of the vulnerability to be exploited (may be non-zero)
- $cost(remediation_{proactive})$: the total cost of the proactive remediation listed in Table 11
- $cost(remediation_{reactive})$: the total cost of the reactive remediation listed in Table 12
- $loss(breach)$: the cost of loss due to security breach listed in Table 12
- $\alpha = \frac{cost(remediation_{reactive})}{cost(remediation_{proactive})}$, assume that reactive remediation is costlier than proactive remediation, a reasonable assumption given the extensive work required to identify, isolate, clean-up and restore affected network sectors.

If the following relation is true, then proactive remediation should be taken.

$$p * \left(\alpha * cost\left(remediaton_{proactive}\right) + loss(breach)\right) > cost(remediation_{proactive})$$

$$loss(breach) > \frac{1 - \alpha p}{p} cost(remediation_{proactive})$$

The above relation indicates that it is advisable to proactively remediate when any of the following conditions is true:

- $loss(breach)$ is greater than $\frac{1-\alpha p}{p}$ $cost(remediation_{proactive})$
- p is large such that the chance of exploitation is almost certain

---

[10] We note here that some risk due to certain vulnerabilities may be so low that it is not worth the time and effort to mitigate.

- α is large (that is the cost of reactive remediation is much higher than that of the proactive remediation)

4.3 SOME OBSERVATIONS ON COST FACTORS

In this section, we make the following general observations with respect to the cost factors of a remediation action:

- Although cost factors of a remediation action can be enumerated, setting their values and combining them into a measure are two distinct tasks, both of which will require some form of human input. Some of the following steps could alleviate the task of human involvement in setting values:
    - Learn from or use historical records
    - Learn from related activities such as incident handling processes
    - Learn from cyber security risk management
    - Keep records of value setting
    - Keep records of value setting rationale

- To alleviate the task of combining cost factors, some of the following steps are worth considering:
    - Quantify and convert cost factors to the same measurement unit
    - Define some methodologies for combining cost factors:
        - A combined value measure may not be adequate due information being lost in the combination process
        - Different aspects of remediation (deployment, operational impact, and risk/loss) may have different orders of magnitude even when converted to the same measurement unit – causing one of them to dominate the others or one to be dominated by others. In combining them together, we lose the proportional weight of each aspect even if they are normalized individually or together
        - It might be beneficial to consider a three-tuple cost measure consisting of (deployment cost, operational impact cost, risk/loss cost), where each tuple can have its own measurement unit, if necessary. Using this measure, we would select a COA based on three-tuple cost threshold consisting of (deployment budget threshold, operational impact budget threshold, and risk/loss budget threshold), where each threshold has its own appropriate value and unit. Having a 3-tuple measure also allows us to focus on the cost component that matter most. For example, from a military perspective, operational impact cost may be more important than the deployment cost.

- Some of the cost factors may contain confidential information or need to be derived using confidential information. This is especially true with respect to the operation impact cost and risk/loss cost. For example, consider the information needed for the following method of deriving operational impact cost:
    - When the system is operating normally, its maximum operating capacity is 100%

  - This 100% capacity is determined based on all personnel having 100% access to all their required services, devices, and information set.
  - Any operational impact cost is due to the loss of operational capacity. Reduced personnel access to their required services, devices, and information results in a loss in operational capacity. This loss reduces the normal maximum operating capacity of 100% to a level that may be unacceptable.

To compute the above operating capacity, we will need the information below which may be confidential.

- Who is using what services, devices, and set of information[11]
- Correlation of the usage and importance of services, devices, and information to mission/organization objectives
- What services, devices, and set of information are affected by a remediation action and to what degree

Similar information such as mission activities and cyber assets is required by Mussman to evaluate the impact of cyber attacks on missions [Mussman-2010].

---

[11] Considering all the relevant cost factors in theory ensures our cost accounting process is complete. In practice, we may be able to get away with a coarser granularity of information detail. This is subject to further investigation.

5. Remediation Cost Revisited

To determine the cost factors for cyber remediation activities, we propose to use a costing methodology referred to as activity and material-based costing (AMBC). This methodology identifies activities and assigns a cost according to actual use/disuse. It also identifies procured materials/equipment and assigns a cost according to actual deployment.

Our proposed approach assumes that

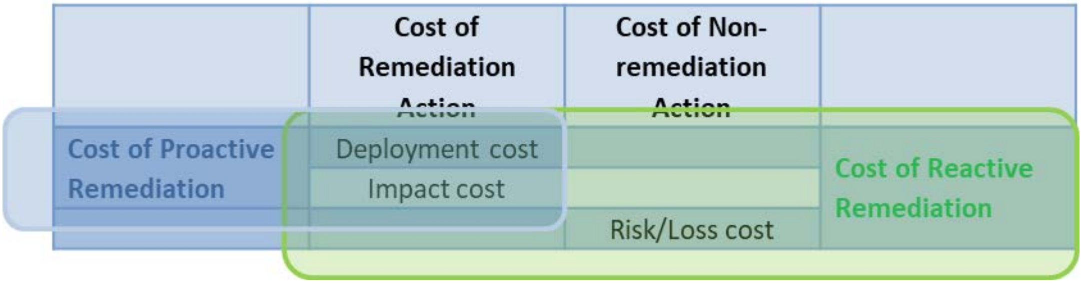
- the list of discovered vulnerabilities is available as a result of the prior-completed vulnerability discovery step
- risk level of vulnerabilities has been determined
- remediation COA for each vulnerability or a group of vulnerabilities has been determined
- selection of which remediation to execute is yet to be determined and thus the need for
    - the list of remediation cost factors
    - the aggregation of the remediation cost factors, and
    - ultimately, the cost of a remediation action

The objective of this section is to list the cost factors of a remediation action for a particular vulnerability. This vulnerability could be a software flaw or a weakness in configuration that allows a system to be compromised. Although the cost of remediation can be categorized in many ways, we find it helpful to consider the one shown in Table 13 that consists of the following three high-level cost components:

- remediation deployment cost
- remediation impact cost
- non-remediation risk/loss cost

Each of the three cost components is defined in the following subsections.

Table 13 Categorization of Remediation Cost



	Cost of Remediation Action	Cost of Non-remediation Action	
Cost of Proactive Remediation	Deployment cost		Cost of Reactive Remediation
	Impact cost		
		Risk/Loss cost	

5.1 REMEDIATION DEPLOYMENT COST

Remediation deployment cost has two subcomponents consisting of labor and material costs. These subcomponents are described in Table 14 and Table 15 below.

5.1.1 Labor Cost

The labor cost due to remediation deployment can be further decomposed according to the deployment phases. Depending on the circumstances, some labor types may not apply or even be required, especially in a scenario where some of the deployment steps are fully automated. In general, each labor cost type can be in a monetary unit based on the respective established labor rate and the amount of time spent. Labor cost is thus evaluated as $cost = time * labor\_rate$.

Table 14 Labor Cost Factors

Labor Type	Cost Factors	Rationale/Comment
Pre-deployment		
• training for the remediation task	• *time* spent by trainer and trainee in training • *labor rate* of trainer and trainee in training	Additional personnel training may be needed to deploy the remediation properly. This labor type may not apply in all cases. For example, new hires or fixing new platform may require this labor type.
• determining the right remediation	• *time* spent in determining which remediation is right • *labor rate* used in doing this task	The right remediation may still have to be determined. If the vulnerability has been identified but there are a number of possible options, some effort is needed to determine the right/better option.
• obtaining or developing the remediation	• *cost* of procuring the remediation or • *time* and *labor rate* used in developing the remediation	The remediation may be readily available but not free, or may not available and has to be developed.
• testing the remediation	• *time* spent in testing remediation • *labor rate* used in doing this task	The remediation has to be tested for effectiveness. If the test can be done automatically, this labor type will not apply.
Deployment		
• notifying affected parties	• *time* spent in notifying affected parties • *labor rate* used in doing this task	The affected parties may have to be notified. If the remediation can be done in the background without any perceptible impact, the labor type will not apply.
• deploying the remediation	• *time* spent in deploying the remediation • *labor rate* used in doing this task	The remediation has to be deployed. If this process is fully automated, then this labor type does not contribute its cost factors to the total deployment cost.

Post-deployment		
• evaluating the remediation	• *time* spent in evaluating the remediation • *labor rate* used in doing this task	The deployed remediation has to be evaluated for correctness and effectiveness. If this evaluation step is fully automated, then this labor type does not apply.
• reporting and/or documenting the remediation	• *time* spent in reporting /documenting the remediation • *labor rate* used in doing this task	What remediation and how the remediation is completed need to be documented.
• rolling back if needed the remediation	• *time* spent in rolling back the remediation • *labor rate* used in doing this task	In case, the remediation is not properly working or installed as expected, rollback may be needed. Otherwise, this labor type does not contribute.

5.1.2 Material Cost

Table 15 Material Cost Factors

Material Type	Cost Factors	Rationale/Comment
Software		
• list of software	*cost* of corresponding software	New software may be needed to complete the remediation task.
Hardware		
• list of hardware	*cost* of corresponding hardware	New hardware may be needed to complete the remediation task such as replacing firewalls.

5.2 REMEDIATION IMPACT COST

The remediation impact cost factors generally identifies the object or user affected, how long the impact is, and the relative importance of the user and affected object. The latter is determined based on the mission priority. The reasons for including each of them are:

- impacted object: reduces the expected functionality of the system
- user: impacted object has to be used or required by some users to count as a contributing cost factor
- time: impacted object takes time to recover, and for different impacted objects and in different scenarios, the recovery time could differ
- mission: system requirement and usage change according to mission objective, emphasizing the importance of different users and services accordingly

These cost factors are presented in Table 16 according to the impacted object types.

Table 16 Remediation Impact Cost Factors

Impact Type	Cost Factors	Rationale/Comment
Services	• *impacted service set,* both directly and indirectly (the more services impacted the higher the remediation cost is likely to be) • *time* to remediate (the longer it takes to remediate, the costlier it can be) • *importance of the impacted service* according to the current mission (the nature of deployment can dictate the value of a service) • *importance of the impacted user* according to the current mission (the circumstance of the users will affect the value of a required service)	Remediation action may impact service availability. To measure the loss of services, we need to know what services are impacted, who are using them, how they are being used, and what the effects of the current mission has on the importance of the services and those using them. With these cost factors of the services, we can have a measure for the loss of services. See Section 5.2.1 for a measure of the loss of services.
Devices	• *impacted device set,* both directly and indirectly (the more devices impacted the costlier it will likely be to remediate) • *time* to remediate (the longer it takes to remediate, the costlier it may be) • *importance of the impacted device* according to the current mission (the nature of its use can dictate the relative value of the device to the current mission) • *importance of the impacted user* needing the device under the current mission (the circumstance of the users will affect the relative value of the device to the user)	Remediation action may impact device availability. To measure the loss of devices, we need to know what devices are impacted, who are using them, how they are being used, and what the effect of the current mission has on the importance of the devices and those using them. With these cost factors of the devices, we can have a measure of the loss of devices. See Section 5.2.2 for a measure of the loss of devices.
Information	• *impacted information set*, both directly and indirectly (the more information impacted the costlier it will likely be to remediate) • *time* to remediate (the longer it takes to remediate, the costlier it will likely be) • *importance of the impacted information* under the current mission (the nature of its use can dictate the relative value of the information to the current mission)	Remediation action may impact information availability. To measure the loss of information, we need to know what information are impacted, who are using them, how they are being used, and what the effect of the current mission has on the importance of the information and those using them. With these information cost factors , we can have a measure of the loss of information. See Section 5.2.3 for a

	• *importance of the impacted user* needing the information under the current mission (the circumstance of the user will affect the relative value of the information to the user)	measure of the loss of information.

In the following Subsections 5.2.1, 5.2.2, and 5.2.3, we propose examples of computing measures for the loss of services, devices, and information, respectively using the cost factors provided in Table 16. Different methods can be used with the cost factors to come up with corresponding measures. Depending on the situation, some factors may be more relevant than others. Section 10 provides a hypothetical service impact cost example and includes related discussion on information and device impact.

5.2.1 A Measure of Loss of Services

We define the following parameters for use in an example to compute cost measures due to service loss:

- R be the set of remediation
- IS_r be the set of impacted services due to remediation $r\epsilon R$
- P be the set of personnel
- $w_{s,m}$ be the weight of the service s under mission m
- $w_{p,s,m}$ be the weight of the personnel p using service s under mission m
- $t_{r,s}$ be the amount of time service s will be impacted due the remediation r
- $U_\sigma(p,s,m,r\ )$ be the loss of service s usage by personnel p for mission m due to the remediation r

We propose the following cost measure for the loss of services due to remediation $r\epsilon R$ for a particular mission m:

$$\sum_{p\in P}\sum\nolimits_{s\in IS_r} U_\sigma(p,s,m,r)$$

where $U_\sigma(p,s,m,r) = w_{s,m} * w_{p,s,m} * t_{r,s}$ is a possible loss of services measure.

5.2.2 A Measure of Loss of Devices

We define the following parameters for use in an example to compute cost measures due to device loss:

- R be the set of remediation
- ID_r be the set of impacted devices due to remediation $r\epsilon R$
- P be the set of personnel
- $w_{d,m}$ be the weight of the device d under mission m
- $w_{p,d,m}$ be the weight of the personnel p using device d under mission m
- $t_{r,d}$ be the amount of time device d will be impacted the remediation r

- $U_\delta(p, d, m, r)$ be the loss of device d usage by personnel p for mission m due to the remediation r

We propose the following cost measure for the loss of device usage due to remediation $r\epsilon R$ for a particular mission m:

$$\sum_{p \in P} \sum\nolimits_{d \in ID_r} U_\delta(p, d, m, r)$$

where $U_\delta(p, d, m, r) = \ w_{d,m} * \ w_{p,d,m} * t_{r,d}$ is a possible loss of device usage measure.

5.2.3 A Measure of Loss of Information

We define the following parameters for use in an example to compute cost measures due to information loss:

- R be the set of remediation
- II_r be the set of impacted information due to remediation $r\epsilon R$
- P be the set of personnel
- $w_{i,m}$ be the weight of information i under mission m
- $w_{p,i,m}$ be the weight of the personnel p using information i under mission m
- $t_{r,i}$ be the amount of time information i will be impacted due to remediation r
- $U_\iota(p, i, m, r)$ be the loss of information i usage by personnel p for mission m due to the remediation r

We propose the following cost measure for the loss of information usage due to remediation $r\epsilon R$ for a particular mission m can be defined as follows:

$$\sum_{p \in P} \sum\nolimits_{i \in II_r} U_\iota(p, i, m, r)$$

where $U_\iota(p, i, m, r) = \ w_{i,m} * \ w_{p,i,m} * t_{r,i}$ is a possible loss of information usage measure.

5.2.4 Converting Time Unit to Monetary Unit

Ordinarily, cost is usually defined as a monetary unit. However, the measures defined in Sections 5.2.1, 5.2.2, and 5.2.3 utilize the unit of time. We show that they can also be converted to monetary units if needed.

We propose a method to convert them to monetary units as an example of standardizing the cost units. To do so, we can define the following additional parameters, respectively for loss of services, devices, and information:

- $r_{p,s}$ is the labor rate of personnel p using service s being impacted under current mission m over the period of remediation;

- $r_{p,d}$ is the labor rate of personnel p using device d being impacted under current mission m over;
- $r_{p,i}$ is the labor rate of personnel p using information i being impacted under current mission m over the period of remediation.

And their respective $U(p,*,m)$s, represented in monetary units, can be defined as follows:

- $U_\sigma(p,s,m) = w_{s,m} * w_{p,s,m} * t_{m,s} * r_{p,s}$
- $U_\delta(p,d,m) = w_{d,m} * w_{p,d,m} * t_{m,d} * r_{p,d}$
- $U_\iota(p,d,m) = w_{i,m} * w_{p,i,m} * t_{m,i} * r_{p,i}$

5.3 NON-REMEDIATION RISK/LOSS COST

A reasonable way to estimate the non-remediated risk/loss cost is to estimate what could be lost when a network is breached. This estimate may be further modified by considering the likelihood of exploitation of a non-remediated vulnerability.

To assist in the risk/loss estimation, we list the cost contributing factors for the non-remediated loss cost in Table 17. A number of the factors may need to be further decomposed with additional info such those from the risk assessment database.

Table 17 Non-remediation Risk/Loss Cost Factors

Loss Type	Cost Factors	Rationale/Comment
Information	In addition to the loss of information availability described above, information loss can appear in one or all of the following forms, each of which may have a different set of refined cost factors: • revenue loss (data being ransomed or data being unavailable to generate more revenue) • loss on intellectual property (cannot be used to litigate or to be more competitive) • damage to brand reputation (resulting in loss in sale or future contract or partnership) • hidden cost (such as requiring data recovery) • future vulnerability (current loss may enable more information loss in the future)	These are some of the additional cost factors that could be associated with information breach.
Reputation	Change in the number of partners, customers, employees, sales, and suppliers	The negative changes in these factors may result in the organization being less competitive and effective.

Trust	• Change in number of business partners, customers, employees, sales, and suppliers • Change advertisement budget	The negative changes in the first set of factors may result in the organization being less competitive. The need for more advertisement budget may deplete budget for other needs such as new security related hardware
Compliance	• Fines for not complying	Fines may be imposed for being non-compliant
Further exploitation	• If a successfully exploited vulnerability generates additional vulnerabilities that could be further exploited, then we need to consider their associated cost factors in coming up with a subtotal cost. • If a successfully remediated exploit generates additional vulnerabilities, then we also need to consider their associated cost factors.	One successful exploit may facilitate more exploits. If they are known, we can recursively determine the non-remediation risk/loss cost factors associated to these exploits.
Financial	• compensation litigation (impacted customer may litigate for compensation) • insurance premium hike (if cyber security insurance is used) • financial theft (if the system handles financial transactions)	Litigation may ensue – requiring subsequent compensation. Insurance, if used, its premium may increase. If financial transactions are being handled, then there is a chance of financial theft loss.

5.4 REACTIVE COST FACTORS

Reactive cost factors will have, in addition to those components described in Sections 5.1, 5.2, and 5.3, the following components that also have a similar cost factor structure as described so far:

- recovery deployment cost
    - In addition to the vulnerability remediation deployment cost, we can also consider a damage recovery deployment cost. For example, instead of software patching, there may be a need to recover data from backup storage.
- recovery impact cost
    - Instead of the impact being due to software patching, the impact could be due to executing the recovery tasks. Table 18 describes the associated impact cost factors in greater detail.
- actual non-remediation risk/loss cost
    - Instead of estimating potential risk/loss cost, we have to calculate what was actually lost.

Table 18 Reactive Recovery Impact Cost Factors

Loss Type	Cost Factors	Rationale/Comment
Services	• See Services entry of Table 16.	Note that the loss of services here is due to the breach not the remediation impact as mentioned in Table 16. To measure the loss of services, we need to know what services are impacted, who are using them, how they are using them, and what the effect of the current mission has on the importance of the services and those using them. With these cost factors of the services, we propose a loss of services measure, an example of which is given in Section 5.2.1.
Devices	• See Devices entry of Table 16.	Note that the loss of devices here is due to the breach not the remediation impact as mentioned in Table 16. To measure the loss of devices, we need to know what devices are impacted, who are using them, how they are using them, and what effect of the current mission has on the importance of the devices and those using them. With these cost factors of the devices, we can have a measure of the loss of devices, an example of which is given in Section 5.2.2.
Information	• See Information entry of Table 16.	Note that the loss of information here is due to the breach and not that of the remediation impact as mentioned in Table 16. To measure the loss of information, we need to know what information is impacted, who is using it, how they are using it, and what the effect of the current mission has on the importance of the information and those using it. With these cost factors of information, we can have a measure of the loss of information, an example of which is given in Section 5.2.3.

5.5 SIGNIFICANCE OF REMEDIATION COST FACTORS

Mitigation is the main objective of a remediation action. However, remediating a functional system could affect its normal operating performance. Thus, a remediation action could have a consequential side effect that may be unavoidable. The cost of these two components (mitigating and impacting) of the remediation action depends on the respective cost factors contributing to each component. Another aspect of mitigation is either avoiding a potential risk or having to recover from a realized risk. The treatment of this risk cost aspect is described in more detail in Sections 5.5.1 and 5.5.2.

The significance of each cost factor to each component, mitigating or impacting, is thus based on its association with that component and its relative contribution to that component. Determining to which component, mitigating or impacting, a cost factor is associated with is easier than to determine its value. The amount/weight will usually depend on the complexity of the specific remediation action and context

Thus a framework that allows for the accounting of the labor and material cost required by the mitigating remediation steps, and the accounting of the impacted set affecting the mission capability and personnel productivity will be beneficial for a specific remediation cost factors evaluation. This will allow analysis of cost factors for any remediation scenario provided the relevant cost factors data are available.

As the significance of a cost factor may be context specific and may not be obvious ahead of time, we need a means to attribute it to the overall remediation cost computation. Sections 5.5.1 and 5.5.2 describe a framework for attributing cost factors in a proactive remediation scenario and a recovery remediation scenario, respectively.

5.5.1 Proactive Remediation Cost Factors

A proactive remediation mitigates vulnerabilities. Thus, if done properly, there should be no cost due to exploited vulnerabilities. In fact when executed, it averts the potential cost due to the vulnerabilities. On the contrary, both deployment and impacted assets incur costs. The costs are due to loss of productivity and effort/material spent.

The significance of the negative cost due to mitigated risk is that its absolute value indicates the severity of the risk it is mitigating. This attribute can be used to select the remediation action based on maximizing risk reduction. The cost of the risk that is reduced will depend not only on the vulnerabilities but also on the context where the vulnerabilities reside. Therefore, some analysis is required to determine the cost and similarly specific cost factors that are involved.

Figure 1 illustrates the effect of executing a proactive Course of Action (COA). As noted above, the cost resulting from proactively mitigating risk due to vulnerabilities is negative. The vulnerabilities affect confidentiality, integrity, and availability of the system at risk. The execution of a COA will take a number of deployment steps, involving preparation, fixing, testing, and reporting. Each step will require effort and may require new material. The total deployment cost is then the sum of all the steps taken. The significance of the deployment cost factors lies in their contributed amounts and associated steps. Associated deployment steps are needed to mitigate while they unavoidably impact the system they are mitigating. Note that some steps, such as the preparatory steps, may not impact at all while the fixing and testing steps usually cause non-negligible, measurable impact. Again, the specific steps depend on the specific remediation action.

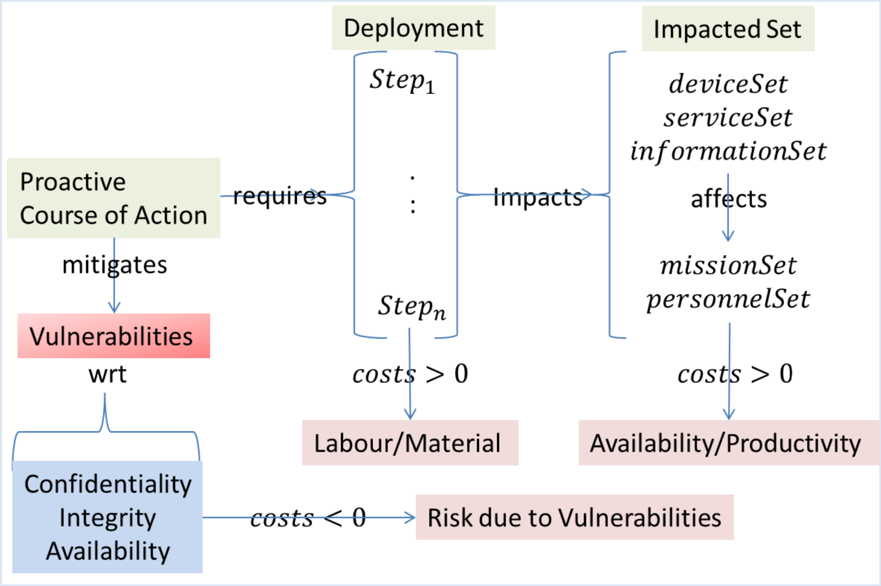


Figure 1 Consequences of a Proactive Course of Action

Also shown in Figure 1 are the two levels of impact. The first level consists of the device, services, and information. Any changes on this level affect the mission performance and personnel productivity which constitute the second impact level. In the proactive case, the main aspect of impact is availability. The impact will be on the system architecture, its operation, and its intended usage. The significance of the associated cost factors is thus how the system architecture, its operation, and its intended usage are affected.

For both deployment and impact set, we seek to minimize the cost but for different reasons. For the former, it is to minimize the effort/material; for the latter, it is the impact on the system capability.

5.5.2 Recovery Remediation Cost Factors

While a proactive remediation mitigates vulnerabilities, a recovery remediation recovers from breaches as shown in Figure 2.

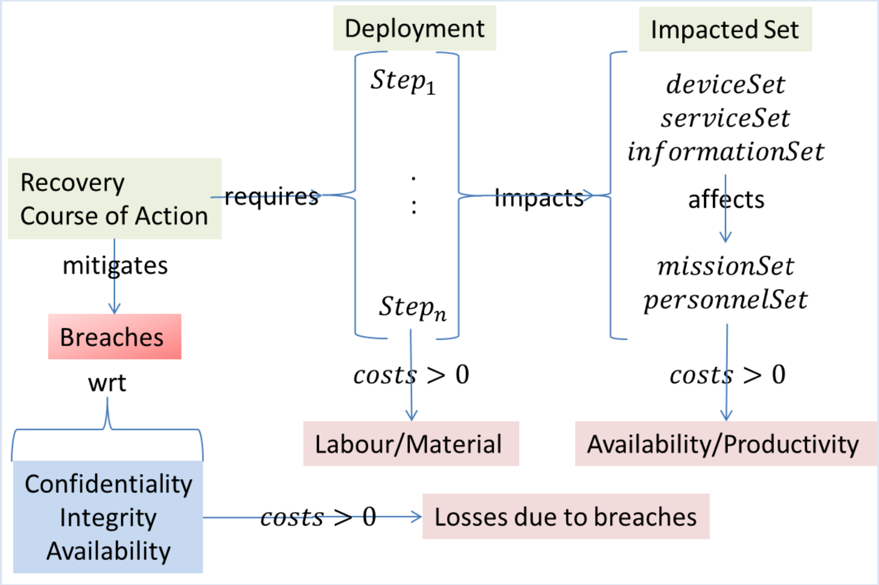


Figure 2 Consequences of a Recovery Course of Action

In the recovery case, one or a combination of confidentiality, integrity, availability components of the system at risk has been breached. In such a case, since vulnerabilities have been exploited and damages occurred and may still be on-going, the cost resulting from losses due to breaches is real and positive. Similarly, both deployment and impacted sets incur positive costs in terms of effort/material and productivity, respectively.

The significance of the losses due to breaches may be the values and the magnitude of various losses. The deeper significance of these losses may have to be interpreted based on the organization's policy and purpose of existence. However, we can analyze the losses based on the aspect of recoverability. Unrecoverable cost, if it exists, is not useful for deciding which recovery actions to take. Examples of unrecoverable costs include loss of life and target opportunity. If this unrecoverable cost can be associated with a vulnerability that has a remediation action, then, this cost value can be used in future proactive remediation decision making.

The recoverable losses will then focus on the extent to which damage can be fixed and/or the extent to which on-going losses can be stopped. This information is useful for deciding which recovery actions to adopt to minimize further loss. To select which recovery action has the minimal effort and impact, we will still need to consider its deployment and impact cost.

Other than what has been discussed above, the significance of the recovery remediation cost factors is similar to that of the proactive remediation cost factors described in Section 5.5.1.

6. Aggregating Remediation Cost Factors

In this section, a methodology for aggregating remediation cost factors is proposed. Firstly, we use a tree structure to illustrate the inter-relationship among cost factors of various abstraction levels. Secondly, we aggregate from the lowest level up to the cost factors subtrees rooted at 'Deployment Cost', 'Impact Cost', and 'Risk of Losses', which are described respectively in Sections 6.1, 6.2, and 6.3. Lastly, we illustrate how the aggregated cost factors could be used to determine proactive/reactive remediation sets that are within budget in Section 6.4. The pros and cons of the proposed aggregation methodology are described in Section 6.5.

Next, we introduce the cost factor tree shown in Figure 3. It is a high-level view of the cost factors tree rooted at 'Reactive Cost'. The figure shows the reactive costs being subdivided into a recovery cost and a proactive cost due to the proactive actions taken to prevent the actions identified in the reactive remediation. The rest of the figure is self-explanatory.

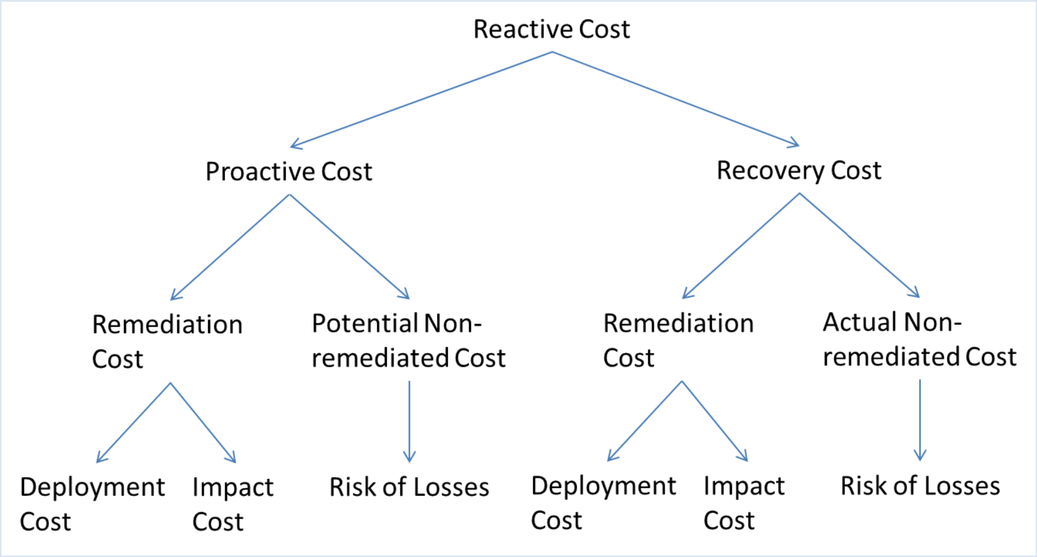


Figure 3 Remediation Cost Factors Tree

When performing proactive remediation, consideration of cost factors below the 'Proactive Cost'/'Remediation Cost' subtree initially appears to be sufficient. However, further reflection indicates that the cost factors below the 'Potential Non-Remediated Cost' could be used to influence the choices of proactive remediation to minimize potential/projected risk/loss. In other words, we can use such factors to decide which proactive remediation action will be of maximum benefit. In this sense, it is similar to the usage of AssetRank [Sawilla-Ou-2008] which assigns rank weights to every vertex in the attack graph. The weight reflects the value of the vertex to the attacker. In the methodology proposed in this section it is to rank remediation actions most beneficial in reducing potential risk. The metric will have to be derived with foresight through a risk assessment process.

The above figure also indicates that in a reactive remediation mode, we will need to consider the cost factors tree rooted at 'Reactive Cost'. There exists an additional 'Recovery Cost' subtree with similar structure as that of the 'Proactive Cost' subtree. The major difference is that its remediation cost is based on the recovery action while non-remediated cost is due to those risks that actually occurred. Thus, its 'Non-Remediated Cost' is no longer a predicted value. It has to be estimated in hindsight. Moreover, its recovery deployment and impact cost are elements in addition to those having been considered in the proactive mode.

In the following subsections, we will describe in more detail the 'Proactive Cost' subtree, define its associated aggregating method, and then an aggregating method for the 'Reactive Cost' tree. The details of the 'Recovery Cost' subtree can be inferred from those of the 'Proactive Cost' subtree and will thus not be described further in this document.

6.1 REMEDIATION DEPLOYMENT COST FACTORS

If we expand the left subtree of Figure 3 showing only the 'Proactive Cost'/'Remediation Cost'/ 'Deployment Cost' subtree portion, we have the subtree shown in Figure *4*.

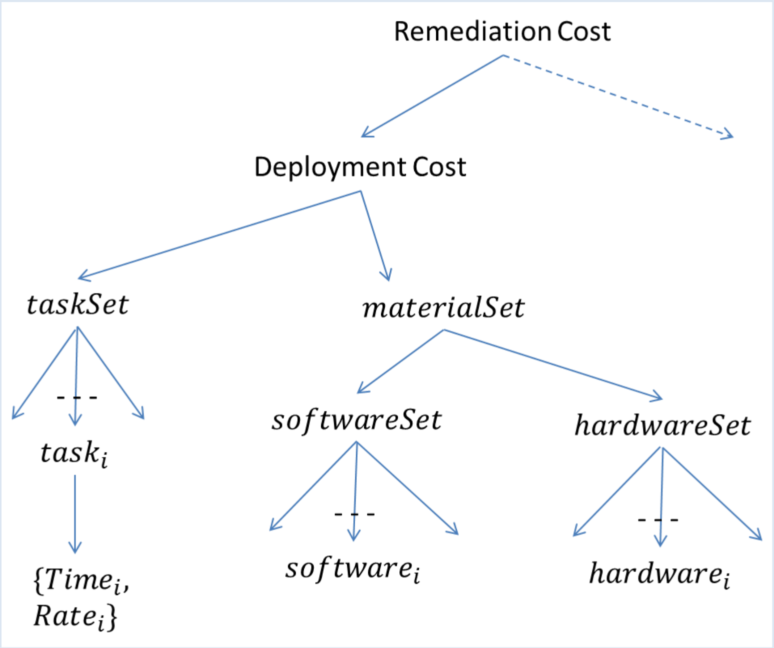


Figure 4 *Deployment Cost Factors Subtree.*

The figure shows that the deployment cost comes from the task and material sets. The task set is a group of activities that must be performed during remediation. The material set is the group of materials that contribute to the deployment costs.

One way to aggregate the remediation deployment cost factors and to compute a total cost is to group them first under the task and material categories. A task is a work item needed in the deployment of a remediation action. It requires time and effort that need to be accounted for. Material is the hardware and software needed for the deployment of a remediation action.

This leads us to having the $taskSet$ performed and $materialSet$ bought. The cost of the $task_i \in taskSet$ can be computed based on $laborRate_i$ and $timeSpent_i$ as follows:

$$cost(task_i) = laborRate_i * timeSpent_i$$

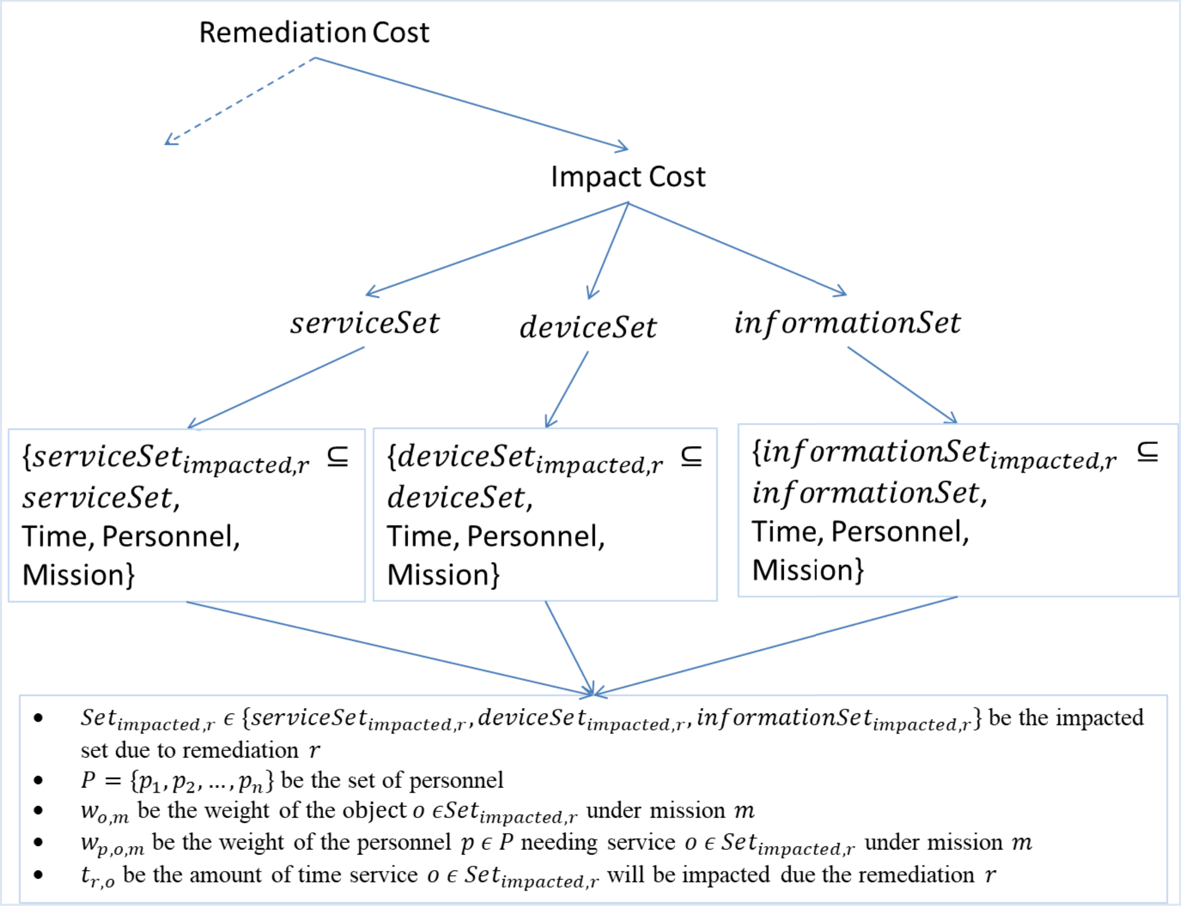
The cost of a remediation deployment that requires a set of tasks, $taskSet$ and a set of materials,$materialSet = \{softwareSet, hardwareSet\}$, is then computed as follows:

$$deploymentCost = \\ \sum_{task_i \in taskSet} cost(task_i) + \\ \sum_{software_i \in softwareSet} cost(software_i) + \sum_{hardware_i \in hardwareSet} cost(hardware_i)$$

Note that the implied unit above is monetary and thus all cost components can simply be added together. The above aggregation method can accommodate any future cost factors that may yet arise.

6.2 REMEDIATION IMPACT COST FACTORS

If we expand the left subtree of Figure 3 showing only the ‘Proactive Cost’/’Remediation Cost’/‘Impact Cost’ subtree portion, we have the subtree shown in Figure 5.


Remediation Cost
Impact Cost
$serviceSet$
$deviceSet$
$informationSet$
$\{serviceSet_{impacted,r} \subseteq serviceSet,$ Time, Personnel, Mission}
$\{deviceSet_{impacted,r} \subseteq deviceSet,$ Time, Personnel, Mission}
$\{informationSet_{impacted,r} \subseteq informationSet,$ Time, Personnel, Mission}

- $Set_{impacted,r} \in \{serviceSet_{impacted,r}, deviceSet_{impacted,r}, informationSet_{impacted,r}\}$ be the impacted set due to remediation r
- $P = \{p_1, p_2, \ldots, p_n\}$ be the set of personnel
- $w_{o,m}$ be the weight of the object $o \in Set_{impacted,r}$ under mission m
- $w_{p,o,m}$ be the weight of the personnel $p \in P$ needing service $o \in Set_{impacted,r}$ under mission m
- $t_{r,o}$ be the amount of time service $o \in Set_{impacted,r}$ will be impacted due the remediation r

Figure 5 Impact Cost Factors Subtree

One way to aggregate remediation impact cost factors and come up with a total cost is to first group them under service, device, and information categories. This leads to consideration of impacts on $serviceSet$, $deviceSet$, and $informationSet$. The following lower-level cost factors characterize the above sets:

- $P = \{p_1, p_2, \ldots, p_n\}$ is the set of personnel
- $Set_{impacted}$ is the impacted set, which is one of $\{serviceSet_{impacted}, deviceSet_{impacted}, informationSet_{impacted}\}$, where
    - $serviceSet_{impacted} \subseteq serviceSet$
    - $deviceSet_{impacted} \subseteq deviceSet$
    - $informationSet_{impacted} \subseteq informationSet$
- t_o is the time that object $o \epsilon Set_{impacted}$ will be impacted due to remediation
- w_o is the importance of the impacted object $o \epsilon Set_{impacted}$
- $w_{p,o}$ is the importance of the user $p \epsilon P$ with respect to the impacted object $o \epsilon Set_{impacted}$

Using the above cost factors, the cost of $Set_{impacted}$, is arrived at by applying the following formula:

$$cost(Set_{impacted}) = \sum_{p \in P} \sum_{o \in Set_{impacted}} U(p, o),$$

where $U(p, o) = w_o * w_{p,o} * t_o$ is a possible loss/cost measure.

The total impact cost is then obtained by the following formula:

$$impactCost = \sum_{Set_{impacted} \epsilon \{serviceSet_{impacted}, deviceSet_{impacted}, informationSet_{impacted}\}} cost(Set_{impacted})$$

Note that the implied unit above is time. It can be converted to a monetary unit by providing a dollar per unit time factor, which could be derived from the personnel labor rate. An example of this conversion is given in Section 5.2.4. If the impact cost is in monetary unit, then it can simply be added to the deployment cost which is already in monetary unit.

Note also that in the above discussion, we assume the impact cost is for a particular remediation r for a system used for a particular mission m. To explicitly include them in the above formulas, we redefine some of the lower-level cost factors as shown below:

- $Set_{impacted,r,m}$ is the impacted set due to remediation r, under mission m which is one of $\{serviceSet_{impacted,r,m}, deviceSet_{impacted,r,m}, informationSet_{impacted,r,m}\}$, where
    - $serviceSet_{impacted,r,m} \subseteq serviceSet$

    - $deviceSet_{impacted,r,m} \subseteq deviceSet$
    - $informationSet_{impacted,r,m} \subseteq informationSet$
- $t_{r,o}$ is the time that object $o \in Set_{impacted,r,m}$ will be impacted due to remediation r
- $w_{o,m}$ is the importance of the impacted object $o \in Set_{impacted,r,m}$ under mission m
- $w_{p,o,m}$ is the importance of the user $p \in P$ with respect to the impacted object $o \in Set_{impacted,r,m}$ under mission m

Using the refined cost factors from above, the refined cost of $Set_{impacted,r}$ under mission m for remediation r, can be obtained via the following formula:

$$cost\left(Set_{impacted,r,m}\right) = \sum_{p \in P} \sum_{o \in Set_{impacted,r,m}} U(p,o,m,r),$$

where $U(p,o,m,r) = w_{o,m} * w_{p,o,m} * t_{r,o}$ is a possible loss/cost measure.

The total impact cost for remediation r for system under mission m is then given as follows:

$$impactCost_{r,m} = \sum_{Set_{impacted} \in \{serviceSet_{impacted,r,m}, deviceSet_{impacted,r,m}, informationSet_{impacted,r,m}\}} cost\left(Set_{impacted}\right)$$

6.3 NON-REMEDIATION RISK/LOSS COST FACTORS

If we expand the right subtree of 'Proactive Cost' in Figure 3 showing only the 'Potential Non-remediated Cost' subtree portion, the resultant subtree resembles the one in Figure 6.

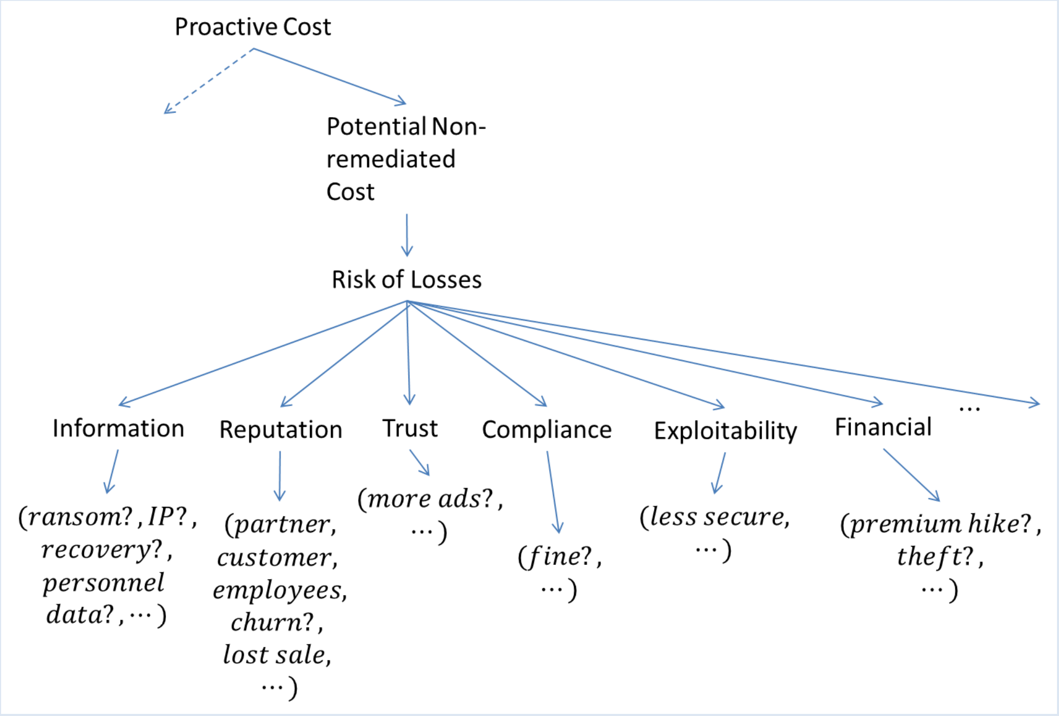

Proactive Cost
Potential Non-remediated Cost
Risk of Losses
Information
Reputation
Trust
Compliance
Exploitability
Financial
…
(ransom?, IP?, recovery?, personnel data?, …)
(partner, customer, employees, churn?, lost sale, …)
(more ads?, …)
(fine?, …)
(less secure, …)
(premium hike?, theft?, …)

Figure 6 Potential Non-remediated Cost Factors Subtree

To aggregate the cost of "risk of losses", we propose to combine its lower level cost factors. Note that most of them could be estimated using a monetary unit. Factors whose cost is not easily estimated in monetary units (e.g. personnel data, churn in partners/ customers/ employees, less security etc) can be converted into monetary units via other methods. For example:

- personnel data cost
    - Let $P = \{p_1, p_2, \dots, p_n\}$ be the set of personnel whose data is breached
    - Let w_p be the importance of personnel p
    - Let c_p be the estimated/assigned cost per personnel p
    - A simple summing formula could be $\sum_{p \epsilon P} w_p * c_p$
- churn cost
    - Let $churnSet = \{partnerSet, customerSet, employeeSet\}$ be the different set of churns
    - Let c_t be the cost of $t \epsilon T$, where $T \epsilon\ churnSet$
    - A simple summing formula would be $\sum_{t \epsilon T} \sum_{T \epsilon churnSet} c_t$
    - Some examples of determining the different churn costs are given below:
        - The cost factors of employee churn could be the cost of hiring, training, coming up to speed, and loss of productivity.
        - The cost factors of partner churn could be the cost of finding new partner, coming up to speed with the partner, and loss of productivity.
        - The cost factors of customer churn could be the cost of finding and retaining new customers, and loss in sale.
- exploitability cost
    - This exploitability cost is due to the additional vulnerabilities introduced by having a non-remediated vulnerability or having had an exploited vulnerability. For this, a security posture metric (SPM) could be used to measure the cost or consequence of such non-remediation. This metric, however, may not be in monetary unit.
    - Another cost measure could be estimating the (deployment and impact) cost of remediating these newly introduced vulnerabilities. This cost measure will now be in monetary unit if we use the aggregating method described in Sections 6.1 and 6.2.

Assuming the cost factors below the ‘Risk of Losses’ subtree in Figure 6 are all computed in monetary units, we can combine them together as described next.

- Let $riskSet = \{informationSet, reputationSet, trustSet,$ $complianceSet, exploitabilitySet, financialSet, \dots\}$ be the set of risk of losses
- Let $cost(t)$ be the cost of $t \epsilon T$, where $T \epsilon\ riskSet$
- A simple summing formula for non-remediation cost could be $\sum_{t \epsilon T} \sum_{T \epsilon riskSet} cost(t)$

Note first of all that future cost factors categories whenever they arise under the ‘Risk of Losses’ subtree in Figure 6 can always be accommodated in the above aggregation method. Moreover, in aggregating costs under each of the above categories, we need to ensure consistency in counting of the lower-level cost factors as well as ensure that they are not double-counted. For example, ransom payment could be a cost due to loss of information or system availability. It could also be considered under financial loss. However, regardless of the method used to count it, it should only be included once under one category. For ease of accounting, it should also be consistently included under the same category. In certain circumstances, some of the cost factors may not apply. For examples, a lost sale opportunity may be an appropriate cost for a commercial enterprise but not for a defense organization, while a failed military mission will be more appropriate for a defense organization.

6.4 APPLICATIONS OF AGGREGATED COST FACTORS

This section describes our proposed aggregation of cost factors and its use in the partitioning of the remediation space. The discussion below applies equally to that of the recovery remediation space.

Ideally, the available budget threshold is sufficiently high that all high risk vulnerabilities above $Risk_{threshold}$ are proactively remediated as shown in Figure 7.

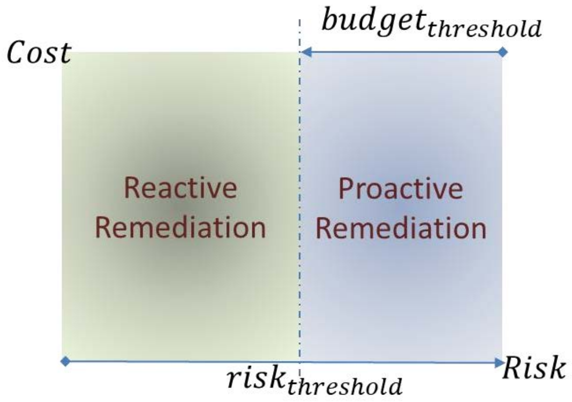


Figure 7 Ideal Partitioning of Remediation Space by Budget and Risk Thresholds

In practice the remediation space will most likely be partitioned in the manner illustrated in Figure 8 based on the allocated budget. If the allocated budget is $Budget_{threshold1}$, which is below the threshold needed to remediate all the risk to the right of $Risk_{threshold}$, then some of risk that should have been mitigated would have remained. On the other hand, if the allocated budget is $Budget_{threshold2}$, then all the risk to the right of $Risk_{threshold}$ would be remediated, including some to the left of it. Ideally, the allocated budget is exactly what is needed to mitigate all the risk to the right of the risk threshold, $Risk_{threshold}$.

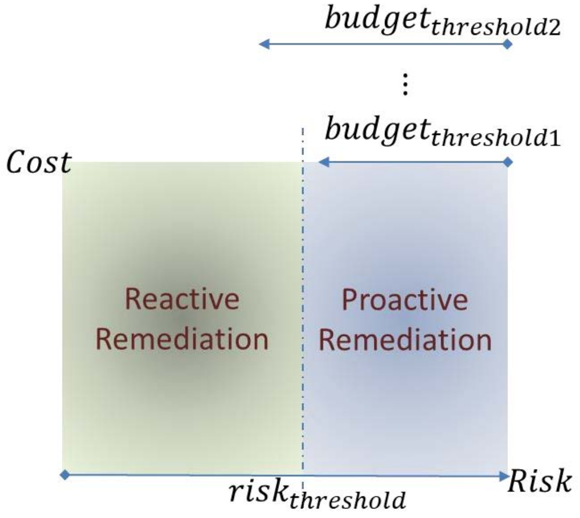


Figure 8 General Partitioning of Remediation Space by Budget and Risk Thresholds

From the above three Subsections, 6.1, 6.2, and 6.3, we arrive at the following three high-level cost factors associated with remediation and non-remediation cost under mission m, which is implicitly assumed henceforth:

- deployment cost for remediation r
    - $deploymentCost_r = \sum_{task_i \,\epsilon\, taskSet_r} cost(task_i) + \sum_{software_i \,\epsilon\, softwareSet_r} cost(software_i) + \sum_{hardware_i \,\epsilon\, hardwareSet_r} cost(hardware_i)$
- impact cost for remediation r
    - $impactCost_r = \sum_{Set_{impacted} \epsilon \{serviceSet_{impacted,r}, deviceSet_{impacted,r}, informationSet_{impacted,r}\}} cost\left(Set_{impacted}\right)$
- cost of risk of losses for not executing remediation r
    - $non\text{-}remediatedCost_r = \sum_{t \epsilon T} \sum_{T \epsilon riskSet_r} cost(t)$

We will use the above cost information to determine a proactive remediation set in Section 6.4.1 and its subset that is within budget in Section 6.4.2. A similar approach will be followed in Section 6.4.3 and Section 6.4.4 for a reactive remediation set.

6.4.1 Determining Proactive Remediation Set

Given a set of remediation actions, $R = \{r_1, r_2, \dots, r_{r_n}\}$ and a risk threshold, $risk_{threshold}$, then the proactive remediation set is given as follows:

$$R_{proactiveSet} = \{r | non\text{-}remediatedCost_r \geq risk_{threshold}, r \,\epsilon\, \{r_1, r_2, \dots, r_{r_n}\}\,\}$$

So far we assume that all $non\text{-}remediatedCost_r$ are equally probable. We can refine the cost value by applying a weight proportional to its probability of occurrence or at its computation of individual lower-level cost factors.

6.4.2 Determining Proactive Remediation Set within Budget

Given a set of proactive remediation actions, $R_{proactiveSet} = \{r_{p1}, r_{p2}, \dots, r_{p_n}\}$ from Section 6.4.1 and a budget threshold, $budget_{threshold}$, then a remediation subset that is below budget is given as follows:

$$R_{\substack{proactive \\ within\ budget}} = \{r | \max\Big(\sum_{r \epsilon R_{proactiveSet}} deploymentCost_r + impactCost_r\Big) \leq budget_{threshold}\}$$

The above formula is subject to various interpretations and thus different implementations. Some of them are briefly discussed below for illustrative purposes:

- The simplest approach is to randomly pick one $r \epsilon R_{proactiveSet}$ at a time; add its $deploymentCost_r + impactCost_{r,m}$ to the cost of the remediation actions selected so far until the running total exceeds the budget threshold, $budget_{threshold}$. Then all the remediation actions selected before the last one form the proactive remediation subset that is within budget.

- Instead of picking randomly, we can elect the remediation $r\epsilon R_{proactiveSet}$ with the highest/lowest $non\text{-}remediatedCost_r$ from among the remaining $r\epsilon R_{proactiveSet}$ until the budget is exceeded.
- We can also select the remediation $r\epsilon R_{proactiveSet}$ with the highest risk first until the budget is exceeded.
- Because we know there are two high-level cost factors, we can also use them to bias our remediation selection process such as selecting $r\epsilon R_{proactiveSet}$ with minimal impact cost first.
- Note also that a combination of the above selection criteria is also possible.

6.4.3 Determining Reactive Remediation Set

Note that the reactive cost has two high-level cost components, proactive cost and recovery cost. Each of the cost components can be computed in the same manner by partitioning the actions into remediating or recovery types. The ‘remediating’ actions, $R = \{r_1, r_2, \dots, r_{r_n}\}$, are actions to remediate vulnerabilities while recovery actions, $\mathrm{P} = \{\rho_1, \rho_2, \dots, \rho_{\rho_n}\}$, are actions to recover from damages done.

Given a set of remediation actions, $R = \{r_1, r_2, \dots, r_{r_n}\}$ and a risk threshold, $risk_{\substack{proactive \\ threshold}}$, then the proactive remediation set is given as follows:

$$R_{proactiveSet} = \{r \mid Potential\ non\text{-}remediatedCost_r \geq risk_{\substack{proactive \\ threshold}}, r \in \{r_1, r_2, \dots, r_{r_n}\}\}$$

Given a set of recovery actions, $\mathrm{P} = \{\rho_1, \rho_2, \dots, \rho_{\rho_n}\}$ and a risk threshold, $risk_{\substack{recovery \\ threshold}}$, then the recovery remediation set is given as follows:

$$\mathrm{P}_{recoverySet} = \{\rho \mid Actual\ non\text{-}remediatedCost_r \geq risk_{\substack{recovery \\ threshold}}, \rho \in \{\rho_1, \rho_2, \dots, \rho_{\rho_n}\}\}$$

So far we assume that all $Potential\ non\text{-}remediatedCost_r$ are equally probable. We can refine the cost value by a weight proportional to its probability of occurrence or at its computation of individual lower-level cost factors. As for $Actual\ non\text{-}remediatedCost_r$, we assume they can be accurately estimated.

Note that depending on the set security policy, $risk_{\substack{recovery \\ threshold}}$ may be equal to $risk_{\substack{proactive \\ threshold}}$. Further investigation is needed to determine the appropriate values for these risk thresholds.

6.4.4 Determining Within Budget Reactive Remediation Set

Given a set of proactive remediation actions, $R_{proactiveSet} = \{r_{p1}, r_{p2}, \dots, r_{p_n}\}$ from Section 6.4.3 and a budget threshold, $budget_{\substack{proactive\\threshold}}$, then a proactive remediation subset that is below budget is given as follows:

$$R_{\substack{proactive\\within\ budget}} = \{r \mid \max(\sum_{r \epsilon R_{proactiveSet}} deploymentCost_r + impactCost_r) \\ \leq budget_{\substack{proactive\\threshold}}\}$$

Given a set of recovery remediation actions, $\mathrm{P}_{recoverySet} = \{\rho_{r1}, \rho_{r2}, \dots, \rho_{r\rho n}\}$ from Section 6.4.3 and a budget threshold, $budget_{\substack{recovery\\threshold}}$, then a recovery remediation subset that is below budget is given as follows:

$$\mathrm{P}_{\substack{recovery\\within\ budget}} = \{\rho \mid \max(\sum_{\rho \epsilon \mathrm{P}_{recoverySet}} deploymentCost_\rho + impactCost_\rho) \\ \leq budget_{\substack{recovery\\threshold}}\}$$

The formulae proposed above are also subject to various interpretations and thus different implementations as described in Section 6.4.2. Note that depending on the set security policy, $budget_{\substack{recovery\\threshold}}$ may be equal to $budget_{\substack{proactive\\threshold}}$. Further investigation is needed to determine the appropriate values for these budget thresholds.

6.5 PROS AND CONS OF THE PROPOSED AGGREGATION METHODS

In this section, we present the general requirement for aggregating cost factors and discuss the pros and cons of the proposed aggregation methodology.

6.5.1 General Requirement of Aggregation Methodology

As with any methodology for combining data, the proposed aggregation methods will require having good understanding of the following to work properly:

- well-defined guidelines for deciding:
  - risk threshold setting
  - budget threshold setting
  - missions priority within a campaign objective
  - activities priority in a mission
  - personnel priority in different context
  - services, devices, information importance
- situational awareness
  - what services, devices, and information are available
  - what are the consequences if some of the services, devices, and information are unavailable
  - how do the services, devices, and information interact with one another
- dealing with value setting of cost factors
  - having sufficient experience and/or sufficient supporting data to come up with reasonably meaningful values based on above guidelines
  - quantifying values and degrees of importance per guidelines
  - accommodating uncertainty in value setting
  - being consistent and repeatable, especially for estimations made by different people in different parts of a large organization and thus the importance of guidelines or standards
  - ensuring no double counting
- learning from related fields and the past
  - incident handling process
    - for the actual non-remediated cost factors
    - data collected in the incident reports
  - risk assessment management
    - for the potential non-remediated cost factors
    - dealing with uncertainty estimation
    - likelihood of occurrence
  - historical data of other organizations or internally collected data from previous remediation activities
- keeping records for future use
  - values setting and associated rationale

6.5.2 Advantages

The proposed aggregation methods based on the bottom-up composition of a cost factors tree have the following advantages:

- the cost factors are organized by how they individually contribute to the higher-level cost factors
    - The lowest level cost factors may not have to be in the same measurement unit. The combined high-level cost factors can be formulated in the same measurement unit, currently in monetary unit.
    - related cost factors are organized to
        - ease understanding of the roles of cost factors
        - allow for drilling down to the different level of the contributing cost factors
        - separate proactive remediation cost from recovery remediation cost
        - separate deployment cost from impact cost
        - cover reactive, proactive, and recovery cost factors in the same aggregation methodology
        - allow for dominant cost factor analysis
        - allow for focusing only on specific cost factors of interest
- high-level cost factors are cast in monetary unit
    - the high-level cost factors needed for decision making are cast in monetary unit and thus provide a better intuitive understanding
- highly extendible/adaptable
    - new cost factors can easily be added as they arise
    - negligible cost factors for a particular scenarios can easily be discounted
- applicable to various scenarios
    - using potential/actual non-remediated cost as a risk measure
    - using the proactive cost factors subtree to determine the proactive remediation set
    - using both the proactive and recovery cost factors subtrees to determine the reactive remediation set
    - using the time cost factors in the impact and deployment cost subtrees for scheduling purpose (a topic requiring more investigation)

6.5.3 Disadvantages

The possible disadvantages associated with the proposed aggregation methods are:

- may take time and experience to set values of cost factors meaningfully
- need to have additional info related to each candidate remediation action
    - task list: the list of tasks to complete the remediation action
    - material list: the list of material required by the remediation action
    - impact on services, devices, personnel, and information on a per mission basis
    - risk due to non-remediation action
- need to be systematic to ensure
    - no-double counting[12]
    - consistency (all values need to be determined consistently)

---

[12] This could be done by defining independent variable or if it is a variable that is used to denote certain cost, each such cost variable instantiation denotes a disjoint cost value,

    - ensuring completeness, that is, all remediation actions have to be evaluated up to the same level of details with respect to the cost factors tree (all cost factors need to be included consistently)
- need to consider uncertainty in
    - estimating cost factor values
    - assessing risk
- need to have a good understanding of
    - service hierarchy, interrelationship, redundancy, how one service affects another or the unavailability of one affects the others
    - missions requirement of personnel, system, and information
    - importance of information for personnel and missions
    - need to know the availability info of services, information, and devices
- need to collect info from multiple sources, a partial list is given below:
    - mission continuity management, counterpart of business continuity management, that maintains and helps develop and tests mission plans and preparations to cope with changes/disasters/delays
    - human resources that know how many employees are involved, what jobs they are doing, how much they are paid, …
    - financial department that paid for what services, devices, …
    - legal/compliance functions that is knowledgeable with penalty, regulations, …

---

7. Validating Remediation Cost Factors

This section describes a set of validation procedures that we propose for the remediation cost factors and its associated aggregation methods based on the results of their practical applications. To make sense of the validation process, we need to define the test conditions, scenarios, and results expectations.

The test conditions could be such that all needed info is given[13]:

- risk threshold
- budget threshold
- courses of action set
- lowest level cost factors such as $task_i = \{laborRate_i, timeSpent_i\}$
- mission related info
- services related info
- devices related info
- task related info
- material related info
- information related info
- personnel related info
- risk related info due to potential/actual non-remediation

The scenarios to consider could be one or a combination of some of the following:

- determine the proactive remediation set within budget
- determine the reactive remediation set within budget
- determine the proactive non-remediated set considering only the risk threshold

The results could be evaluated in one or all of the followings aspects:

- with respect to the cost factors
    - Do the proposed cost factors make sense?
    - What cost factors would an SME consider for selecting proactive/reactive remediation action set?

---

[13] Considering all the relevant information ensures our test conditions will be accurate. In practice, it may be sufficient to utilize only the key information. Determining this subset needs further investigation as it may be context-specific.

Initially, some of the information may have to be estimated by SMEs based on their knowledge and experience. Over time, if these estimates are recorded systematically with their corresponding rationale, we will be able to build on them and obtain more accurate estimates.

Some of information may depend on the organizational policies and guidelines such as risk and budget thresholds that are considered acceptable. Labor rate, personnel information, and material related information may be available from the accounting and human resources departments. Mission, services, and information related information may be available from the operational department. Once the sources of information are determined, it is then just a matter of establishing the channels, ideally automated ones, to access them.

- with respect to the proposed aggregation methods
    - How would a SME do the aggregation, and does the aggregation make sense?
- with respect to the applications of the aggregation methods
    - Do the results obtained in using the proposed cost factors make sense?
    - How do the results compare with known formulae?
    - How do the results compare with what an SME would have done?

8. Research Conclusion

In this work, we have identified and listed all the factors that influence remediation costs. We subdivided the cost factors into categories representing the types of costs they would contribute to. Network defenders can use these cost factors to determine measures that represent remediation effort and assist in situational awareness and decision making. As part of this work, we propose methods to aggregate the factors to determine the cost measures. Our proposed approaches include mathematical formulae and factor trees. We also present methods, which we did not test, that could be used to validate the aggregation methods. We defer rigorous research on aggregation methodologies and their validation, which were beyond the scope of this work, to possible future work.

8.1 RECOMMENDATIONS

The cost factors tree indicates that taking proactive action could be more cost effective than taking reactive action which entails additional recovery cost. Instead of adding the non-remediation cost to the deployment cost, we suggest using it to partition the remediation actions space. We also propose considering the cost measure to have the following three basic cost components:

- deployment cost
- impact cost
- risk cost

Each of the above cost components has a distinct associated budget, as indicated below, that we need to manage.

- financial budget – amount of money and effort to spend
- capability/productivity budget – amount of productivity, objective, and mission to miss or not
- risk budget – amount of risk to take or not

Moreover, we recommend applying the cost factors tree for cost accounting of real scenarios. We believe being able to automate the lower-level cost factors collection and computation will facilitate further investigation and deployment of the cost factors tree.

It should be noted that there are different defence scenarios and use cases where different factors would be suitable, and others would be inappropriate. Cost factors are not necessarily all rolled up into a single cost metric, but relevant factors can be selected to represent a required cost metric. For example, deployment costs would hardly be relevant in cases where the problem cannot be correctly solved by "deploying a firewall”. We suggest that algorithms that take this into consideration should be explored when these cost factors are applied. We also suggest investigating how to populate the cost factors tree with scenario and use case specific information.

Since this task did not require us to conduct experiments, we did not investigate the independence of the cost factors. We recommend investigation into cost metric algorithms which account for the interdependencies of the cost factors.

8.2 FUTURE WORK

Some areas related to the applications and refinement of cost factors are listed below:

- explore the use of various information available in cost factors tree (See Section 13 for some more detailed usage examples)
    - use the time component of the cost factors for scheduling purposes especially in a dynamically evolving situation such as the one described in [Mussman-2010] or to minimize the total time needed to complete a set of remediation actions
    - investigate having component-wise thresholds such one for deployment cost and another one for impact cost would result in a more relevant proactive remediation set
    - find optimal solutions for determining the remediation set within budget as formulated in Sections 6.4.2 and 6.4.4
    - integrate with a vulnerability management process [Qualys-2004]
    - determine the dominant cost factors based on historical data
    - start collecting relevant data for populating the cost factors tree
    - with the contributing cost factors explicitly accounted for and readily available, a more sophisticated evaluation of remediation actions becomes possible such as selecting one that requires less time or one that does not impact this service and even one that satisfies a combination of different constraints or conditions
- explore the use of interval arithmetic for specifying cost interval of COA recommendation actions, and budget and risk thresholds
- explore the use of probability with confidence interval for estimating risk cost value as recommended by [Hubbard-2016]
- investigate how to set/extract/derive/update/compute various cost factors value automatically in various operating situations of the computer network system
    - learning from past experience and others' experience
    - learning from related areas such as incident handling and risk assessment
    - coordinating with others affected departments
    - having an organized view of service hierarchy, device interdependency, and personnel service and service requirement based on mission objective
- investigate cost factor value setting in a multiple missions scenario
- investigate issues of uncertainty
    - imperfect or incomplete information
    - discounted operational interdependencies
    - changes in adversarial characteristics
    - undetected vulnerabilities

8.3 SUMMARY

Existing literature in the area of attack graph solutions, intrusion detection solutions, network security, and risk assessment are surveyed for their use of a cost measure. Specifically we examine how cost factors are defined and used for measuring deployment, service impact, and risk estimation costs. These cost factors are then categorized based on remediation consequences and modes. Using the described categories, we suggest refining the deployment cost to consist of labor and material costs, impact cost to consist of loss of services, devices, and information costs, and risk cost to consist of the cost when the remediation action is followed through or not. The categorization according to modes consists of proactive and reactive modes. To aggregate cost factors, we suggest using the cost factors tree that accounts for all the contributing factors. The suggested aggregating method starts from the bottom-up for the different subtrees defining deployment, impact, proactive, recovery, and reactive costs. To validate, we propose to define the conditions, scenarios and expected results, which are based on reasonableness of obtained results, its comparison with existing solutions, and its comparison with SME results. In conclusion, we suggest and describe how to use the cost factors tree and its aggregation methods. We also list future research topics to expand and enhance the applications of cost factors tree. They include, but are not limited to, applying the cost factors tree to real scenario and investigating the suggested aggregation method and verification method for their utility and enhancement.

9. References

[Albanese-2012] M. Albanese, S. Jajodia, and S. Noel, “Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs,” 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 1-12, 2012.

[Armour-COA] Preliminary Research Investigation Report: Course of Action Selector Ver. 0.4, 2015.

[Bhattacharya-2011] P. Bhattacharya and S. K. Ghosh, “Analytical framework for measuring network security using exploit dependency graph,” IET information Security, 2012, vol. 6, issue 4, pp. 264-270.

[Bistarelli-2006] S. Bistarelli, F. Fioravanti, and P. Peretti, “Defense trees for economic evaluation of security investments,” Proceedings of the First International Conference on Availability, Reliability and Security, 2006, pp. 416–423.

[Boddy-2005] M. Boddy,J. Gohde, T. Haigh, and S. Harp, “Course of Action Generation for Cyber Security Using Classical Planning,” Proc. 15th International Conference on Automated Planning and Scheduling, June 5-10, 2005, pp. 12-21.

[Buede-2005] D.M. Buede, “Assignment of Weights,” https://web.stevens.edu/ses/me/fileadmin/me/Monte_Carlo_Process/Class_Lectures/lec1-assigning_weights.ppt

[Butler-2002] S.A. Butler, “Security Attribute Evaluation Method: A Cost-Benefit Approach,” http://www.cs.cmu.edu/~shawnb/SAEM-ICSE2002.pdf

[Chen-2004] P. Chen, M. Dean, D. Ojoko-Adams, H. Osman, L. Lopez, and N. Xie, “Systems quality requirements engineering (square) methodology: Case study on asset management system,” Technical Report, Carnegie Mellon University/Software Engineering Institute, 2004.

[Chen-2008] Chen, F. L. Wang, and J. Su, “An Efficient Approach to Minimum-Cost Network Hardening Using Attack Graphs,” The Fourth International Conference on Information Assurance and Security, 2008.

[Cherdantseva-2016] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, “A review of cyber security risk assessment methods for SCADA systems,” Computer & Security 56 (2016) pp. 1-27.

[Cremonini-2005] M. Cremonini and P. Martini, “Evaluating Information Security Investments from Attackers Perspective: the Return-on-Attack (ROA),” 2005 Fourth Workshop on the Economics of Information Security.

[Deng-2000] H. Deng, C.H. Yeh, R.J. Willis, "Inter-company comparison using modified TOPSIS with objective weights," Comput. Oper. Res. 27 (2000), 963–973.

[Dewri-2007] R. Dewri, N. Poolsappasit, I. Ray, and D. Whitley, D. "Optimal security hardening using multi-objective optimization on attack tree models of networks," 2007 14th ACM Conference on Computer and Communications Security (CCM), pp. 204-213.

[ENISA-2012] European Network and Information Security Agency, "Introduction to Return on Security Investment," December 2012, https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport

[Gaffney-2001] J. Gaffney Jr, and J. Ulvila, "Evaluation of intrusion detectors: A decision theory approach," In 2001 Proc. IEEE Symposium on Security and Privacy, pp. 50–61.

[GD-CONOPS-2014] General Dynamics Canada, "System Concept of Operations (CONOPS) for the Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Contract", DRDC-RDDC-2014-C78, Mar 2014.

[GD-ARMOUR-TD-2015] General Dynamics Mission Systems -- Canada, "Automated Computer Network Defence Technology Demonstration Project Detailed Design Document for the Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Contract", DRDC-RDDC-2016-C133, Oct 2015.

[GITTA-2006] Geographic Information Technology Training Alliance, "Weighting by rating," http://www.gitta.info/Suitability/en/html/Normalisatio_learningObject2.html

[Gordon-2002] L. Gordon and M. Loeb, "The Economics of Information Security Investment," ACM Transactions on Information and System Security, 2002, pp. 438–457.

[Grimaila-2007] M. R. Grimaila, L.W. Fortson, "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," Proc. 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications, pp. 206-212.

[Homer-2009] J. Homer, and X. Ou, "SAT-solving approaches to context-aware enterprise network security management," IEEE JSAC Special Issue on Network Infrastructure Configuration, Vol. 27 (3), pp. 315-322, 2009.

[Hubbard-2016] D.W. Hubbard, R. Seiersen, D.E. Geer Jr., and S. McClure, “How to Measure Anything in Cybersecurity Risk,” John Wiley & Sons, July 25, 2016.

[Hwang-1981] C.L. Hwang, K.L. Yoon, “Multiple Attribute Decision Making: Methods and Applications,” Lecture Notes in Economics and Mathematical Systems, vol. 186, Springer, New York, 1981.

[Idika-2009] N. C. Idika, B. H. Marshall, B. K. Ghargava, “Maximizing Network Security Given a Limited Budget,” Tapia’09, April 1-4, 2009, Portland, Oregon, USA, http://web.ics.purdue.edu/~brandeis/idika-marshall-bhargava-tapia09.pdf

[Ingols-2009] K. Ingols, M. Chu, R. Lippmann, S. Webster, and S. Boyer, “Modeling Modern Network Attacks and Countermeasures Using Attack Graphs,” ACSAC '09 Annual Computer Security Applications Conference, 2009, pp. 117-126.

[Islam-2008] T. Islam and L. Wang, “A Heuristic Approach to Minimum-Cost Network Hardening Using Attack Graph,” NTMS '08, New Technologies, Mobility and Security, 2008, Tangier, Morocco.

[Ismail-2018] N. Ismail, “The financial impact of data breaches is just the beginning,” http://www.information-age.com/data-breaches-financial-impact-123470254/

[Jha-2002] S. Jha, O. Sheyner, and J. Wing, “Two formal analyses of attack graphs,”2002 Proceedings of the 15th IEEE Computer Security Foundations Workshop, pp. 49–63.

[Jajodia-2011] S. Jajodia, S. Noel, P. Kalapa, M. Albanese, J. Williams, “Cauldron, Mission-Centric Cyber Situational Awareness with Defense in Depth,” MILCOM, Military Communications Conference - MILCOM, pp. 1339-1344, 2011

[Kao-2010] C. Kao, “Weight Determination for Consistently Ranking Alternatives in Multiple Criteria Decision Analysis,” Applied Mathematical Modelling, Volume 34, Issue 7, July 2010, Pages 1779-1787.

[Kaspersky Lab] Kaspersky Lab, “DAMAGE CONTROL: THE COST OF SECURITY BREACHES IT SECURITY RISKS SPECIALREPORT SERIES,” https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

[Keramati- M. Keramati, H. Asgharian, A. Akbari, “Cost-Aware Network

2011] Immunization Framework for Intrusion Prevention", International Conference on Computer Applications and Industrial Electronics, pp. 321-326, 2011.

[Keramati-2012] M. Keramati, and A. Akbari, "An Attack Graph Based Metric for Security Evaluation of Computer Networks," (IST'2012), 6'th International Symposium on Telecommunications.

[Kheir-2009] N. Kheir, H. Debar, N. Cuppens-Boulahia, F. Cuppens, J. Viinikka, "Cost evaluation for intrusion response using dependency graphs," IFIP International Conference on Network and Service Security (N2S), IEEE, Paris, France, 2009, pp. 1-6.

[Kheir-2010] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, and H. Debar, "A Service Dependency Model for Cost-Sensitive Intrusion Response," ESORICS 2010: Computer Security – ESORICS 2010, pp. 626-642.

[Kijsanayothin-2010] P. Kijsanayothin and R. Hewett, "Analytical Approach to Attack Graph for Network Security," 2010 International Conference on Availability, Reliability and Security, pp. 25-32.

[Kotenko-2012] I. Kotenko and A. Chechulin, " Common Framework for Attack Modeling and Security Evaluation in SIEM Systems," 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, pp. 94-101.

[Kumar-2016] S.S. Kumar, "Cost Benefit Analysis in Intrusion Detection System," International Research Journal in Global Engineering and Sciences. (IRJGES), Vol. 1, No. 2, July, 2016.

[Lai-1994] Y.J. Lai, T.Y. Liu, C.L. Hwang, "TOPSIS for MCDM," Eur. J. Oper. Res. 76 (1994), 486–500.

[Lala-2001] C. Lala and B. Panda, "Evaluating Damage from Cyber Attacks: A Model and Analysis," IEEE Trans. Systems, Man, and Cybernetics-Part A: Systems and Humans, Vol. 31, No. 4, July 2001, pp. 300-310.

[Lee-2002] W. Lee, W. Fan, M. Miller, S. Stolfo, and K. Jallad, C. Park, E. Zadok, and V. Prabhakar, "Toward cost-sensitive modeling for intrusion detection and response, " J. Comput. Secur. 10, 1–2 (July 2002), pp. 5–22. https://mice.cs.columbia.edu/getTechreport.php?techreportID=274&format=pdf&

[Lippmann-2006] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham, "Validating and Restoring Defense in Depth Using

Attack Graphs," Military Communications Conference, 2006. MILCOM 2006. IEEE MILCOM, 2006, pp: 1- 10.

[Malczewski-1999] J. Malczewski, "GIS and Multicriteria Decision Analysis," 1999. New York: John Wiley & Sons.

[MDA] MDA, Design document for the technology demonstration of the Joint Network Defence and Management System (JNDMS) Project, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc199/p539152_A1b.pdf

[Mercuri-2003] R. Mercuri, (2003), "Analyzing Security Costs," Communications of the ACM, 46(6).

[Mussman-2010] S. Mussman, A. Temin, M. Tanner, D. Fox, and B. Pridemore, "Evaluating the Impact of Cyber Attacks on Missions," MITRE, July, 2010, https://pdfs.semanticscholar.org/70fa/a7b3afa6f3afad7e64b92391d6e968b201ca.pdf

[Nakhla-2017] N. Nakhla, K. Perrett, and C. McKenzie, "Automated Computer Network Defence using ARMOUR," International Conf. on Cyber Situational Awareness, Data Analytics and Assessment, June 2017.

[NIST SP 800-30-2012] NIST, "Guide for Conducting Risk Assessments," Special Publication 800-30, Rev. 1, Sept. 2012.

[Noel-2003] S. Noel, S. Jajodia, B. O'Berry, and M. Jacobs, "Efficient Minimum-Cost Network Hardening Via Exploit Dependency Graphs," Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003).

[Noel-2009] S. Noel, S. Jajodia, B. O'Berry, and M. Jacobs, "Minimum-Cost Network Hardening," U. S. Patent 7,555,778, awarded June 30, 2009.

[Noel-2010] S. Noel, S. Jajodia, L. Wang, and A. Singhal, " Measuring Security Risk of Networks Using Attack Graphs," International Journal of Next-Generation Computing, vol. 1, no. 1, July 2010, pp. 135-147.

[Ou-2005] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: A Logic-based Network Security Analyzer," 14th USENIX Security Symposium (2005).

[Pamula-2006] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A weakest-adversary security metric for network configuration security analysis," 2006 Proceedings of the 2nd ACM workshop on Quality of Protection, pp. 31–38.

[Parnell-2009] G. Parnell and T. Trainor, "Using the Swing Weight to Weight Multiple Objectives," Proceedings of the INCOSE International Symposium, Singapore, July 19-23, 2009. http://www.academia.edu/7973507/Swing_Weight_Matrix

[Pendleton-2016] M. Pendleton and T. Garcia-Lebron, "A Survey of Systems Security Metrics," ACM Computing Surveys, Vol. 49, No. 4, December 2016, pp. 62.1-62.35.

[Ponemon Institute LLC] Ponemon Institute LLC, "2017 Cost of Data Breach Study Global Overview," https://www.ibm.com/security/data-breach

[Poolsappasit-2012] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, Jan/Feb 2012, pp. 61-74.

[Qualys-2004] "Guide to Effective Remediation of Network Vulnerabilities," https://www.qualys.com/docs/guide_vulnerability_management.pdf

[Roszkowska-2013] E. Roszkowska, "Rank Ordering Criteria Weighting Methods – a Comparative Overview," Optimum, Studia Ekonomiczne, https://www.researchgate.net/publication/280081585_Rank_Ordering_Criteria_Weighting_Methods_-_A_Comparative_Overview

[Saaty-1980] T.L. Saaty, "The Analytic Hierarchy Process: Planning Setting Priorities, Resource Allocation," 1980. New York: McGraw-Hill International.

[Saeid-2011] M. Saeid, A.A.A. Ghani, and H. Selemat, "Rank-Order Weighting of Web Attributes for Website Evaluation," The International Arab Journal of Information Technology, Vol. 8, No. 1, January 2011.

[Saha-2016] S. Saha, A.K.S. Vullikanti, M. Halappanavar, and S. Chatterjee, "Identifying vulnerabilities and hardening attack graphs for networked systems", 2016 IEEE Symposium on Technologies for Homeland Security (HST), pp. 1-6.

[Sarlis-2018] P. Sarlis, "Report: Vulnerability Remediation, An Enterprise View of Cost Factors in the Defence Organizational Context," May 2018.

[Sawilla-Burrell-2009] R. Sawilla and C. Burrell, "Course of action recommendations for practical network defence," Technical Memorandum, DRDC Ottawa, TM 2009-130, August 2009.

[Sawilla-Burell-2010] R. Sawilla and C. Burrell, "Metrics-based Computer Network Defence Decision Support," Information Systems and Technology Panel (IST) Symposium, Tallinn, Estonia, November 2010.

[Sawilla-Ou-2008] R. Sawilla and X. Ou, "Identifying Critical Attack Assets in Dependency Attack Graphs," Proceedings of the 13th European Symposium on

Research in Computer Security, pp. 18–34, 2008.

[Schmeider-2016] N. Schmeidler, “Cyber Security – Know Your ROI: Making the Business Case for Cyber Security,” http://engage.morphisec.com/cyber-security-know-your-roi-ebook

[Smith-2017] D. A. Smith, “Vulnerability Remediation: 5 Steps Toward Building an Effective Process,” https://www.beyondtrust.com/blog/vulnerability-remediation-5-steps-toward-building-effective-process/

[Sritapan-2011] V. Sritapan, W. Stewart, J. Zhu, and C.E.T. Rohm, Jr., “Developing a Metrics Framework for the Federal Government in Computer Security Incident Response,” Communications of the IIMA. 11.2 (Aug. 2011): pp. 55-73.

[Stakhanova-2012] N. Stakhanova, C. Strasburg, S. Basu, S., and J.S. Wong, “Towards Cost-sensitive Assessment of Intrusion Response Selection,”, J. Comput. Secur. 20, 2–3 (2012), 169–198, https://pdfs.semanticscholar.org/c2e7/c822a536864faaae8db67db75ec4aeb4a380.pdf

[Stolfo-2000] S. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. Chan, “Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project,” In 2000 Proc. DISCEX’00. pp. 130–144.

[Strasburg-2009b] C. Strasburg, N. Stakhanova, S. Basj, and J.S. Wong, “Intrusion Response Cost Assessment Methodology,” ASIACCS’09 Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, March 10-12, 2009, pp. 388-391.

[Task TA 004] Statement of Work (SOW) for Task TA 004 – Remediation Factors to Support Determination of a Remediation Cost Measure

[theamegroup] the ame group, “Data Security Breach: 5 Consequences for Your Business,” https://www.theamegroup.com/security-breach/

[Vandenberghe-2007] G. Vandenberghe, “Visually Assessing Possible Courses of Action for a Computer Network Incursion,” SANS Institute InfoSec Reading Room http://www.sans.org/reading-room/whitepapers/threats/visually-assessing-courses-action-computer-network-incursion-1786

[Wang-2006]. L. Wang, S. Noel, and S. Jajodia, “Minimum-cost network hardening using attack graphs,” Computer Communications, 29 (18). 2006, pp. 3812-3824.

[Wang-2008] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, “An Attack Graph-Based Probabilistic Security Metric,” 2008 Proceedings of the 22nd

Annual Conference on Data and Applications Security, pp. 283–296.

[Wang-2013] S. Wang, Z. Zhang, Y. Kadobayashi, “Exploring attack graph for cost-benefit security hardening: A probabilistic approach,” Computer & Security 32 (2013) pp. 158-169. (http://www.sciencedirect.com/science/article/pii/S0167404812001496)

[Wei-2001] H. Wei, D. Frinke, O. Carter, and C. Ritter, “Cost-Benefit Analysis for Network Intrusion Detection Systems,” CSI 28th Annual Computer Security Conference, October 29-31, 2001, Washington, D.C.

10. Appendix A: A Hypothetical Service Impact Cost Example

An example of service impact cost is described here. In this scenario, we assume there are number of services but only four of them are impacted by three remediation actions. However, each remediation action affects different subset of services. We also assume there are only two personnel affected, each with different associated service requirement weights. Note that with no loss of generality, we limit the number of personnel, remediation actions, and impacted services for ease of illustration.

Although the nature of the mission could affect the weights of services and personnel, we assume they have been set accordingly for each mission. So for different missions, the same weight variable could have different values. For the following discussion, we are concerned with differentiating the cost of different remediation actions within a particular mission.

Next, we define the problem and then present an example with specific value setting of the cost factors.

Let us define the following parameters for an example of computing the loss of services:

- $S = \{s_1, s_2, s_3, s_4, \ldots\}$ be the set of services
- $R = \{r_1, r_2, r_3\}$ be the set of remediation
- $IS_1 = \{s_1\}$ be the set of services impacted by remediation r_1
- $IS_2 = \{s_4\}$ be the set of services impacted by remediation r_2
- $IS_3 = \{s_2, s_3\}$ be the set of services impacted by remediation r_3
- $P = \{p_1, p_2\}$ be the set of personnel
- $w_{s,m} \geq 1$ be the weight of the service s under mission m
- $w_{p,s,m} \geq 1$ be the weight of the personnel p using service s under mission m
- $t_{r,s}$ be the amount of time service s will be impacted due to remediation r
- $U_\sigma(p, s, m, r)$ be the loss of service s usage by personnel p for mission m due to remediation r

$$cost(r_i) = \sum_{p \in P} \sum_{s \in IS_i} U_\sigma(p, s, m, r_i),$$

where $U_\sigma(p, s, m, r) = w_{s,m} * w_{p,s,m} * t_{r,s}$

As we are only considering two personnel $\{p_1, p_2\}$, the cost for remediation r_i can be expanded as follows:

$$cost(r_i) = \sum_{s \in IS_i} U_\sigma(p_1, s, m, r_i) + \sum_{s \in IS_i} U_\sigma(p_2, s, m, r_i)$$

The cost for each of the remediation r_i is then given as follows:

- $cost(r_1) = \begin{array}{c} U_\sigma(p_1, s_1, m, r_1) + U_\sigma(p_2, s_1, m, r_1) \\ w_{s_1,m} * w_{p_1,s_1,m} * t_{r_1,s_1} + w_{s_1,m} * w_{p_2,s_1,m} * t_{r_1,s_1} \\ w_{s_1,m} * (w_{p_1,s_1,m} + w_{p_2,s_1,m}) * t_{r_1,s_1} \end{array}$

- $cost(r_2) = \begin{array}{c} U_\sigma(p_1, s_4, m, r_2) + U_\sigma(p_2, s_4, m, r_2) \\ w_{s_4,m} * w_{p_1,s_4,m} * t_{r_2,s_4} + w_{s_4,m} * w_{p_2,s_4,m} * t_{r_2,s_4} \\ w_{s_4,m} * (w_{p_1,s_4,m} + w_{p_2,s_4,m}) * t_{r_2,s_4} \end{array}$

- $cost(r_3) =$
  $U_\sigma(p_1, s_2, m, r_3) + U_\sigma(p_2, s_2, m, r_3) + U_\sigma(p_1, s_3, m, r_3) + U_\sigma(p_2, s_3, m, r_3)$
  $w_{s_2,m} * \left(w_{p_1,s_2,m} + w_{p_2,s_2,m}\right) * t_{r_3,s_2} + w_{s_3,m} * (w_{p_1,s_3,m} + w_{p_2,s_3,m}) * t_{r_3,s_3}$

Next, we apply the above formulas to describe the impact cost factors and their contribution to the remediation cost in a hypothetical scenario. Let the set of impacted service set be {Email, Database, Voice, Web} as given in Table 19. The time $t_{r,s}$ for remediation r and the importance of impacted services $w_{s,m}$ and users $w_{p,s,m}$ are also given. The computed cost for each remediation action r_i is presented by the colored $cost(r_i)$ entry. Its color matches those of the contributing cost factors. Note that for different missions, the assigned weights will be different.

Table 19 Example of an Impact Cost Computation

Cost Factors	Email (s_1)	Database (s_2)	Voice (s_3)	Web (s_4)
$w_{s_i,m}$	2	3	4	1
$w_{p_1,s_i,m}$	2	2	3	1
$w_{p_2,s_i,m}$	2	3	2	2
t_{r_1,s_i} (time)	2	0	0	0
t_{r_2,s_i} (time)	0	0	0	2
t_{r_3,s_i} (time)	0	.5	1	0
$cost(r_1) = w_{s_1,m} * \left(w_{p_1,s_1,m} + w_{p_2,s_1,m}\right) * t_{r_1,s_1} = 16$				
$cost(r_2) = w_{s_4,m} * \left(w_{p_1,s_4,m} + w_{p_2,s_4,m}\right) * t_{r_2,s_4} = 6$				
$cost(r_3) = w_{s_2,m} * \left(w_{p_1,s_2,m} + w_{p_2,s_2,m}\right) * t_{r_3,s_2} + w_{s_3,m} * (w_{p_1,s_3,m} + w_{p_2,s_3,m}) * t_{r_3,s_3}$ $7.5 + 20$				

If the Database service is supposed to provide information that is important to the current mission and it is not accessible, then we would have a loss of information usage cost component. Loss of information is also possible through loss of connection. If any of the aforementioned situations occur, the loss can be computed as shown above for the loss of service. Otherwise, there will be no loss of information cost component.

Similarly, if there are devices that have to be taken down or replaced, we will have the loss of device usage cost if they are needed in the current mission. Its computation will also follow a procedure similar to the one described above for the loss of service. Otherwise, there will be no loss of device usage cost component.

11. Appendix B: Templates for Organizing the Cost Factors of a Remediation Action

Since a remediation action has many cost factors, we need to account for them consistently in an organized fashion. In this section, we present sample templates to record and organize the following associated cost factors:

- those that arise in the process of deployment (Section 11.1)
- those that arise due to the deployment impacts on the object sets being used by personnel for a particular mission (Section 11.2)
    - the device set
    - service set
    - information set

Assuming the cost factors of a remediation action are fully accounted and properly set, we present a mean of computing the total cost of executing a remediation action on a system being used by personnel for multiple missions. The costs for different remediation actions can similarly be evaluated. These results can then be used to determine the set of remediation actions that are within budget.

11.1 DEPLOYMENT COST FACTORS TEMPLATE

To remediate, we need to perform one or more tasks to complete the remediation action. Each task will have a number, description, labor rate, and required time to complete as shown in Table 20.

The cost of each task is shown in the fifth column of the table. The total remediation deployment cost is as shown at the bottom of the table. Note that the deployment does not include its impact costs which are described in the Section 11.2.

Table 20 Deployment Cost Factors Template

Task #	Task Description	Labor Rate ($rate$)	Required Time ($time$)	$cost = rate_i * time_i$
1	$description_1$	$rate_1$	$time_1$	$cost_{task_1}$
2	$description_2$	$rate_2$	$time_2$	$cost_{task_2}$
:	:	:	:	:
n	$description_n$	$rate_n$	$time_n$	$cost_{task_n}$
$cost_{deployment} = \sum_1^n cost_{task_i}$				

11.2 IMPACT COST FACTORS TEMPLATE

A generic template for accounting impacted set is presented in Section 11.2.1. It is then applied to device set, service set, and information set as described within the same section. If object sets of new categories are found to have been impacted, they can similarly be accounted for.

11.2.1 Impacted Set Cost Factors Template for a Mission

A mission generally requires the involvement of personnel - see Table 21 - and resource objects required by the personnel to accomplish the mission - see Table 22. Remediation deployment actions can cause a resource object to become unavailable and thus create a resource impact cost which needs to be computed. To determine the impact cost of a resource, we need to know the role of the resources with respect to the personnel in accomplishing the mission. The associated cost factors of resource j as shown in Table 22 are:

- tl_{obj_j}, time of unavailability
- $mw_{j,m}$, importance with respect to the mission m
- $pw_{i,j,m}$, need by personnel i to accomplish mission m

The loss of resource j can thus be expressed as $mw_{j,m} * pw_{i,j,m} * tl_{obj_j}$. The total cost for the loss of o resources is shown at the bottom of Table 22.

Table 21 Personnel List Template

Personnel pl_i	Personnel Description
1	$description_1$
2	$description_2$
:	:
ϕ	$description_\phi$

Table 22 Impacted Resource Object Cost Factors Template

Object #	Object Description	Time Loss	Mission (m) Importance	Personnel Importance			
				pl_1	pl_2	..	pl_ϕ
1	$description_1$	tl_{obj_1}	$mw_{1,m}$	$pw_{1,j,m}$, for $1 \leq j \leq o$	$pw_{2j,m}$, for $1 \leq j \leq o$	:	$pw_{\phi,j,m}$, for $1 \leq j \leq o$
2	$description_2$	tl_{obj_2}	$mw_{2,m}$				
:	:	:	:				
o	$description_n$	tl_{obj_o}	$mw_{o,m}$				
$cost_{object_m} = \sum_{i=1}^{i=\phi} \sum_{j=1}^{j=o} mw_{j,m} * pw_{i,j,m} * tl_{obj_j}$							

Next we consider the resources of following categories for a given mission m:

- device set
- service set
- information set

Their respective templates are presented in Table 23, Table 24, and Table 25.

Table 23 Impacted Device Set Cost Factors Template

Device #	Device Description	Time Loss	Mission (m) Importance	Personnel Importance			
				pl_1	pl_2	..	pl_ϕ
1	$description_1$	tl_{dev_1}	$dw_{1,m}$	$pdw_{1,j,m}$, for $1 \le j \le \delta$	$pdw_{2j,m}$, for $1 \le j \le \delta$	:	$pdw_{\phi,j,m}$, for $1 \le j \le \delta$
2	$description_2$	tl_{dev_2}	$dw_{2,m}$				
:	:	:	:				
δ	$description_\delta$	tl_{dev_δ}	$dw_{\delta,m}$				
$cost_{device_m} = \sum_{i=1}^{i=\phi} \sum_{j=1}^{j=\delta} dw_{j,m} * pdw_{i,j,m} * tl_{dev_j}$							

Table 24 Impacted Service Set Cost Factors Template

Service #	Service Description	Time Loss	Mission (m) Importance	Personnel Importance			
				pl_1	pl_2	..	pl_ϕ
1	$description_1$	tl_{ser_1}	$sw_{1,m}$	$psw_{1,j,m}$, for $1 \le j \le \sigma$	$psw_{2j,m}$, for $1 \le j \le \sigma$	:	$psw_{\phi,j,m}$, for $1 \le j \le \sigma$
2	$description_2$	tl_{ser_2}	$sw_{2,m}$				
:	:	:	:				
σ	$description_\sigma$	tl_{ser_σ}	$sw_{\sigma,m}$				
$cost_{service_m} = \sum_{i=1}^{i=\phi} \sum_{j=1}^{j=\sigma} sw_{j,m} * psw_{i,j,m} * tl_{ser_j}$							

Table 25 Impacted Information Set Cost Factors Template

Information #	Information Description	Time Loss	Mission (m) Importance	Personnel Importance			
				pl_1	pl_2	..	pl_ϕ
1	$description_1$	tl_{dat_1}	$iw_{1,m}$	$piw_{1,j,m}$, for $1 \le j \le \iota$	$piw_{2j,m}$, for $1 \le j \le \iota$	:	$piw_{\phi,j,m}$, for $1 \le j \le \iota$
2	$description_2$	tl_{dat_2}	$iw_{2,m}$				
:	:	:	:				
ι	$description_\iota$	tl_{dat_ι}	$iw_{\iota,m}$				
$cost_{data_m} = \sum_{k=1}^{k=\phi} \sum_{j=1}^{j=\iota} iw_{j,m} * piw_{k,j,m} * tl_{dat_j}$							

11.2.2 Templates for Multiple Missions

From the above templates, we can compute the remediation cost for a mission as follows:

$$cost_{COA_m} = cost_{deployment} + cost_{service_m} + cost_{device_m} + cost_{data_m}$$

For multiple missions, we will need one personnel list template, and a set of device, service, and information templates for each mission, and one deployment template. The cost for μ number of missions is derived using the following formula:

$$total_{COA_{1..\mu}} = cost_{deployment} + \sum_{m=1}^{\mu} cost_{service_m} + cost_{device_m} + cost_{data_m}$$

Note that the deployment cost is accounted only once and the impact cost is for each mission m that is impacted.

12. Appendix C: Some Weight Setting Formulas

Other than the mission and personnel importance, all cost factors of a remediation action appear straightforward to determine. There are many ways to determine the mission and personnel weights as indicated in Section 11 Appendix B. Some of them are briefly described in this section for future references.

- weighting by ranking (Section 12.1)
- weighting by rating (Section 12.2)
- weighting by pairwise comparison (Section 12.3)

Note that no discussion is made here on the appropriate weight setting method to use. That is left for further investigation. However, a non-exhaustive list of other methods is given in Section 12.4 and a few comparative studies are given in Section 12.5.

The weight setting problem is thus defined as follows. Given n attributes, $A_1, \ldots A_n$, determine the corresponding weights $w_1, \ldots, w_n$, assuming A_i is more important than A_j for $i < j, 1 \leq i \leq n, 1 \leq j \leq n,\ i \neq j$, and the rank of 1 is higher than $i > 1$. In the following discussion, we assume for $1 \leq i \leq n$, attribute A_i has a rank of i.

12.1 WEIGHTING BY RANKING

Using the three rank order weighting formulas as described in [Saeid-2011], we have the followings:

- Rank sum
    - $w_{rs_i} = \frac{n+1-i}{\sum_{j=1}^{n} j} = \frac{2*(n+1-i)}{n*(n+1)}, i = 1, \ldots, n$
- Reciprocal of the rank
    - $w_{rr_i} = \frac{\frac{1}{i}}{\sum_{j=1}^{n} \frac{1}{j}}, i = 1, \ldots, n$
- Rank-order centroid
    - $w_{roc_i} = \frac{1}{n} \sum_{j=i}^{n} \frac{1}{j}, i = 1, \ldots, n$
- Rank exponent [GITTA-2006, Buede-2005]
    - $w_{re_i} = \frac{(n+1-i)^p}{\sum_{j=1}^{n} (n+1-j)^p}, i = 1, \ldots, n, p \geq 0$
    - $w_{re_i} = \frac{1}{n}, p = 0$
    - $w_{re_i} = w_{rs_i}, p = 1$
    - p is an undefined measure of the dispersion in the weights

For each of the above formulas, all weights sums to one ($\sum_{j=1}^{n} w_j = 1$).

Though popular because of the ease of using weighting by ranking, “its explanatory power decreases quickly with an increasing number of criteria. The results of this approach should be interpreted cautiously and documented carefully. They may be used as a first approximation only. [GITTA-2006]”

12.2 WEIGHTING BY RATING

Considering the same problem as above and before computing the weight, we give here the ranked attributes a score according to their relative importance [GITTA-2006] based preferably on experience and historical data as follows:

- Point allocation
  - From a total score of 100, distribute a score to each attribute according to its importance such that score $s_i, s_i \geq s_j, 1 \leq i \leq n, 1 \leq j \leq n, i \neq j$ is given to A_i if A_i is more or equally importance as A_j
  - $\sum_{i=1}^{n} s_i = 100$
- Ratio estimation
  - From a range of value, distribute a score to each attribute according to its importance such that score $s_i, s_i \geq s_j, 1 \leq i \leq n, 1 \leq j \leq n, i \neq j$ is given to A_i if A_i is more or equally important as A_j
  - $\sum_{i=1}^{n} s_i$ can be any arbitrary value

The weights for the above rating are then given by the following formula:

$$w_i = \frac{s_i}{\sum_{i=1}^{n} s_i}$$

Again the ease of their application makes the above formula popular. "It is particularly suitable for problems with a few simple criteria whose relative importance can be estimated with common sense or expertise. However, the distribution of the scores is again subjective and often only poorly justified. [GITTA-2006].

12.3 WEIGHTING BY PAIRWISE COMPARISON

This weighting method is based on the Analytic Hierarchy Process, a decision-making framework, developed by Saaty [Saaty-1980]. It consists of three main steps:

- Forming a square comparison matrix for storing the pairwise relative importance value of A_i compared to A_j for $1 \leq i \leq n, 1 \leq j \leq n$. This matrix M is set with the following values:
  - Setting the diagonal of the matrix. $M_{ii} = 1, 1 \leq i \leq n$
  - Setting the upper right triangular matrix. For relative importance value in the range of 1 to 9, where a value of 9 means very important and 1 means not very important, $M_{ij} = v \,\epsilon \{1, \dots, 9\}$, according to how much A_i is more important compared to A_{ij} for $1 \leq i \leq n, i < j \leq n$. Similarly, for relative importance value in the range of 1 to $\frac{1}{9}$, where a value of $\frac{1}{9}$ means the least important and $\frac{1}{2}$ means not as much important, $M_{ij} = v \,\epsilon \left\{\frac{1}{2}, \dots, \frac{1}{9}\right\}$, according to how much A_i is less important compared to A_{ij} for $1 \leq i \leq n, i < j \leq n$.

  - Setting the lower left triangular matrix. $M_{ji} = \frac{1}{M_{ij}}$, for $1 \le i \le n, i < j \le n$
- Calculating the weight matrix W and weight w_i for A_i $1 \le i \le n$.
  - $W_{ij} = \frac{M_{ij}}{\sum_{k=1}^{n} M_{ik}}$, for $1 \le i \le n, 1 \le j \le n$
  - $w_i = \frac{\sum_{j=1}^{n} W_{ij}}{n}$, for $1 \le i \le n$
  - $\sum_{j=1}^{n} w_i = 1$, as these weights are already normalized
- Assessing matrix consistency.
  - Malczewski [Malczewski-1999] provides "a statistically reliable estimate of the consistency of the resulting weights" [GITTA-2006]
  - Roszkowska [Roszkowska-2013] provides an example.
  - More details on this aspect is left for future investigation.

12.4 OTHER WEIGHT SETTING METHODS

We provide here a non-exhaustive list of other weight setting methods.

- Balance Beam Approach [Buede-2005]
  - This method not only ranks the attribute but also accounts for their relative importance.
- Swing Weight Matrix [Parnell-2009]
  - Similar to Balance beam approach but also considers variation of the range of the attribute.
- TOPSIS (Technique for Order Preference by Similarity to an Ideal Solution) [Hwang-1981] and its variations [Lai-1994, Deng-200]
  - This technique orders preference by similarity to an ideal solution.
- [Kao-2010]
  - This technique uses relative distance derived from the alternative position to the anti-ideal and the ideal alternative to obtain consistent ranking.

12.5 COMPARATIVE STUDIES OF WEIGHTING METHODS

We provide here a non-exhaustive list of comparative studies of weighting methods.

- Roszkowska [Roszkowska-2013] compares equal weights, rank sum, rank exponent, and centroid weights.
- [GITTA-2006] describes the pros and cons of weighting by ranking, weighting by rating, and weighting by pairwise comparison
- Kao [Kao-2010] compares their proposed solution with TOPSIS

13. Appendix D: Sample Usages of Cost Factors Tree

To make the most of the cost factors tree in evaluating the cost of a remediation action, we need to understand more of its underlying components consisting of the following:

- deployment cost
- impact cost
- loss cost

Although we can add the cost together with some weights when they all are in the same unit, we lose a lot of information with respect to what we are minimizing or maximizing. Instead of having a point on a line, it is more informative to have a point in a multi-dimensional space. Thus, from these three components perspective, it makes better sense to treat them as a three-tuple entity as shown in Figure 9.

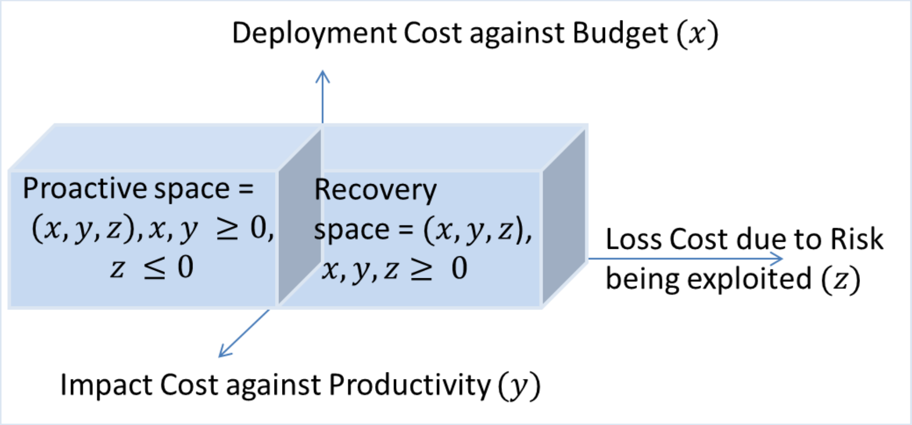

Deployment Cost against Budget (x)
Proactive space = $(x, y, z), x, y \geq 0,$ $z \leq 0$
Recovery space = $(x, y, z),$ $x, y, z \geq 0$
Loss Cost due to Risk being exploited (z)
Impact Cost against Productivity (y)

Figure 9 Cost Factors Space

In Figure 9, deployment cost, impact cost, and loss cost are orthogonal and they can be depicted in three orthogonal axes (x, y, z). This is because each component deals with different kind of budgetary limits as listed below:

- deployment cost uses up financial budget
- impact cost uses up productivity and capability budget
- loss cost uses up risk budget

From Figure 9, we can explain easily the roles of cost factors:

- The subspace consisting of $(x, y, z), x \geq 0, y \geq 0, z \leq 0$ forms the proactive mode space. The loss cost is zero or negative because it is only a potential loss due to risk that has not yet been breached.

- The subspace consisting of $(x, y, z), x \geq 0, y \geq 0, z \geq 0$ forms the recovery mode space. Unlike for the proactive mode, the loss cost here is zero or positive because it is due to risk that has been breached, which may still be on-going.
- The subspace consisting of $(x, y, z), x \geq 0, y \geq 0, z \leq 0$ and $z \geq 0$ forms the reactive mode space.
- The subspace consisting of $(x, y, z), x = 0, y = 0, z \leq 0$ forms the non-remediation space. Here no deployment cost and impact cost are incurred but may have non-negligible loss cost due to potential risk.
- The point $(0, 0, 0)$ is the best place to be. No deployment cost, impact cost, and loss cost of both positive and negative types.
- Each axis is associated with a cost factors subtree as follows:
    - x-axis with the deployment cost factors subtree
    - y-axis with the impact cost factors subtree
    - z-axis with the risk of loss cost factors subtrees

We leave to future investigation on how to describe acceptable cost in the above coordinate system.

Next, we describe some of the usages of the information associated with the cost factors tree.

13.1 GENERAL USE OF COST FACTORS TREE

The remediation mode determines how and what components of the cost factors tree are to be used. The reactive mode will have two sub-modes consisting of the proactive mode and the recovery mode as depicted in Figure 3. Thus, it suffices for us to just explain proactive mode and recovery mode separately.

In the proactive mode, the potential non-remediated cost should be used to select the list of remediation actions to consider based on their contribution to reducing the potential non-remediated cost. Once this set of remediation action candidates is chosen, we can then screen them based on the available financial budget and impact budget. Various methods for doing so are left for future investigation.

Similarly in the recovery mode, the actual non-remediated cost should be used to select the list of remediation actions to consider based on their immediate needs to be mitigated. The loss here has occurred. The urgency here is what must be recovered. Once this set of recovery action candidates is chosen, we can then screen them further as we do for the proactive mode. Various methods for screening them are also left for future investigation.

13.2 USING MULTIPLE COST FACTORS THRESHOLDS

As described earlier, we can treat the cost factors as a three-tuple entity. In this case, we will need a three-tuple threshold consisting of the followings:

- financial budget
- productivity and capability budget
- loss budget

Each tuple here can have different unit, provided the financial budget has the same unit as that of the deployment cost; the productivity and capability budget has the same unit as that of the impact cost; and the loss budget has the same unit as that of the loss cost.

13.3 SIMPLIFYING COST FACTORS EVALUATION

In some situation it may be possible to simplify cost computation. Assuming impact cost is more important than deployment cost, we may just use the cost based solely on impact cost. Another situation is when we do not need very low level details of the cost. In this case, we may be able to forgo the computation below a certain level of the cost factors tree.

13.4 SYSTEM REDUNDANCY TO REDUCE IMPACT COST

If a system that requires fixing is mirrored, then the impact of that system being down is inconsequential. In this case, one of those redundant systems can be serviced one at a time with minimal impact cost.

13.5 OPTIMIZING THE TIME COMPONENT OF COST FACTORS

The time component appears in both the deployment and impact cost factors. In the deployment aspect, time is spent to remediate; while in the impact aspect, time is wasted waiting for the remediation to complete. Therefore, it will be advantageous to do the followings with the time component:

- minimize the amount of time needed, therefore the amount of time wasted
- schedule the remediation period at a time when the impacted services, devices, and information are at their lowest demand
- parallelize the remediation subtasks such that the total transpired time is less than the sum of the sequential times needed for the subtasks and thus minimizing the total down time
- parallelize the remediation subtasks that impact related services, devices, and information rather than for unrelated ones, thus minimizing the unproductive period
    - An example is when both e-mail software and e-mail sever may have to be patched. In this case, patching them at the same time will shorten the total outage time. Of course, if the mail system can be made redundant, then this scenario may not need to be that time-efficient.

14. Appendix E SME Report

The content of the following pages in this appendix is the report of Peter Sarlis on “Report: Vulnerability Remediation, An Enterprise View of Cost Factors in the Defence Organizational Context”. It is a review of the cost factors listed in Section 5 with an attempt to introduce additional relevant cost factors borne from operational experience.

REPORT: VULNERABILITY REMEDIATION

An Enterprise View of Cost Factors in the Defence Organizational Context

Abstract

This report summarizes findings as they relate to a review of documentation developed on behalf of Defence Research and Development Canada (DRDC). The report is in support of the Preliminary Research Investigation Report – a Preliminary Cost Factor List. All work pertains to the DRDC ARMOUR system, whose aim is to "automate computer network defence".

Peter Sarlis

peter.sarlis@ispratis.com

Status: DRAFT

CONTENTS

INTRODUCTION

This report summarizes findings as they relate to a review of documentation developed on behalf of Defence Research and Development Canada (DRDC). The report is in support of the Preliminary Research Investigation Report – a Preliminary Cost Factor List [1]. All work pertains to the DRDC ARMOUR system [2], whose aim is to "automate computer network defence".

BACKGROUND

In approximately December of 2014, Solana Networks and General Dynamics Missions - Canada (GDMS-C) partnered to help develop the DRDC Armour Technology Demonstrator - Automated Computer Network Defence System. Since that time, the ARMOUR project has progressed with several components of the system under continued, iterative development.

In 2018, Solana Networks drafted a "Preliminary Research Investigation Report" whose purpose was to list preliminary cost factors as they relate to the remediation of information system vulnerabilities. These cost factors are intended - in turn - to provide critical inputs to inform the Course of Action (CoA), which can then support automation of CoA prioritization. As part of the ongoing development effort, the preliminary cost factors have undergone additional scrutiny by the project team to better define and refine the presumed cost factors involved in vulnerability remediation.

OBJECTIVE

Per the meeting held on April 20th, 2018 at the Solana Networks Moodie Drive location, DRDC and Solana representatives emphasized:

1. The need for a review of the proposed cost factors;
2. A desire to introduce additional relevant cost factors borne from operational experience; and
3. Cost factors that can be measured from real data.

REMEDIATION COST

PROPOSED HIGH-LEVEL COMPONENTS

In the preliminary report [1], three high-level cost components are identified:

1. Remediation deployment cost;
2. Remediation impact cost; and
3. Non-remediation risk/loss cost.

Of the three high-level cost components identified, the first two - remediation deployment and impact cost - represent components that more closely approach real costs considered by security practitioners willing to publicly share their observations.

PATCH MANAGEMENT

It is important to note that based on experience and the reference material gathered, remediation of vulnerabilities as it relates to patch management tends to be a more documented and discussed component of remediation costs. This may be for several reasons; however, one of the most likely is that the impact of patch management on corporate IT budgets represents a relatively low "return on investment". Patching systems tends to be very expensive, given the high resource costs. However, cyber security best practices consider the adoption of patch management as a crucial element of continuous vulnerability management, thus highly valued as an effective loss-prevention measure.

Since patching systems tends to be a common preventive control for any modern cyber security program, it would likely represent a good portion of any remediation cost factor devised. Consider one possible breakdown of work associated with a typical patching cycle:

- Obtain the patch from a trusted party and validate the patch and source integrity;
- Test the patch to ensure the vulnerability is remediated and the patch will not break other applications – a lengthy and laborious process;
- Notify affected parties of unscheduled downtime (if needed);
- Deploy patch;
- Test post-deployment operational efficiency; and
- Rollback and remediate if needed.

Consider this proposed formula as well [3]:

$$\text{Total Annual Patching Cost} = [(\text{Cost of Patching Event}) \times (\text{Number of Patching Events})] + [(\text{Prepare and Detect Costs}) \times (\text{Number of reported vulnerabilities})] + (\text{Total Annual Ongoing Costs})$$

The "cost of patching event" can be further broken down thus:

$$\text{Cost of Patching Event} = (\text{Fully Burdened Hourly Rate}) \times (\text{Hourly Effort})$$

If we assume that preparation and detection costs include assessment, assembly and testing, deployment, failure resolution, and help desk, the hourly effort of - for example – end-point patching is around 8 hours per system per year. With this relatively simple formula, it would be fair to conclude that a typical enterprise can experience six-figure costs. These conclusions, which are fairly accepted by the practitioner community as typical costs, contribute to the promotion of embedded security practices in the software and system development lifecycle, since doing so in practice lowers the cost of patching after the software and system is deployed into production.

VULNERABILITY CHARACTERISTICS

The various characteristics of a vulnerability can have a direct impact on remediation costs, thus may be considered a cost factor. One broadly adopted method that captures the principle characteristics of a vulnerability is the National Institute of Standards and Technology (NIST) Common Vulnerability Scoring System (CVSS) [4]. The CVSS "provides an open framework for communicating the characteristics and impacts of IT vulnerabilities." It is a quantitative model, which is well suited to meet the requirement to have the cost factors be measurable and numerical.

The latest version of the CVSS (v3.0) is made up of 22 metrics which together formulate a score that can be represented as a vector string. The Temporal metric group includes a metric referred to as "Remediation Level" (RL). This metric can be leveraged to further refine the cost factors. With CVSS v3.0, the RL metric level is defined below. Added to the table are two additional columns; they are "Remediation Cost" and "Rationalization". The table follows:

Metric Value	Description	Remediation Cost	Rationalization
Not Defined (X)	Assigning this value to the metric will not influence the score. It is a signal to a scoring equation to skip this metric.	Unknown	NA
Unavailable (U)	There is either no solution available or it is impossible to apply.	Very High	Since there is no solution available, or the difficulty level to apply a solution is high enough to be cost prohibitive, any attempts to remediate the vulnerability may require extensive labour (research, development, testing), expensive changes to existing systems, and the introduction of new systems, thus lead to very high costs.
Workaround (W)	There is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability.	High	Although an unofficial workaround has been developed, the potential labour costs associated with the development of the workaround are absorbed by the enterprise as opposed to the vendor. Testing the solution may lack appropriate levels of assurance, thus lead to unexpected outcomes (unauthorized and/or accidental changes, unplanned outages).
Temporary Fix (T)	There is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround.	Low	Costs are contained to impact assessment and testing. Some additional cost may be absorbed by the enterprise in the case where a temporary fix is followed by one or more additional temporary fixes before a final, complete solution is available.

Official Fix (O)	A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available.	Very Low	Costs are contained to impact assessment and testing.

INDIRECT COSTS

Although arguably less relevant to this discussion, some vulnerability and asset characteristics are worth mention due to their potential impact to remediation costs. Various considerations are offered below:

- Attack Complexity - In the case where a vulnerability is assumed to be applicable within an enterprise environment, attack complexity may influence the probability a vulnerability may be exploited. Given a scenario where an enterprise is presented with a choice to expend resources to remediate a vulnerability, they may be more willing to expend those resources if the probabilities of exploitation are higher.
- Security Categorization - The security objectives associated with the confidentiality, integrity, and availability of corporate assets may directly influence the resource allocation to vulnerability remediation. In the case where a security category of a defined business activity and process is established at higher levels for confidentiality, integrity, or availability, and the vulnerability associated with the remediation effort exposes the business activity to exploitation, the enterprise may be willing to allocate additional resources to the remediation, regardless if a fix or workaround is available.

FINAL THOUGHTS

REVIEW OF OBJECTIVES

There were three defined objectives for this report:

1. The need for a review of the proposed cost factors;
2. A desire to introduce additional relevant cost factors borne from operational experience; and
3. Cost factors that can be measured from real data.

A review of the proposed cost factors as stipulated in the main reference [1] was conducted. To view the proposed cost factors under a different "lens", a corporate IT enterprise view was taken. Although the proposed cost factors are thorough and very well defined, the methodology used to determine the cost factors is known to be complex and costly to implement in corporate environments. It is unclear if corporate enterprise IT service teams in the public or private sector have used this same methodology to control and measure costs. In the allotted time used to produce this report to conduct open and closed source research, and based on corporate enterprise experience, this has yet to be witnessed in the enterprise. This would suggest that real data to support well defined yet complex cost factors may be especially difficult to find.

Since the limited open source research and extensive corporate experience support the tenuous conclusion that real data may be difficult to acquire, this report attempts to introduce more practical - yet simplistic - approaches to measured remediation costs. Additional time devoted to deeper research - perhaps to include interviews with large corporate entities that may capture data in this space - may be required to discover additional practical methods IT service providers use to support their internal governance structures. An attempt has been made to introduce practical approaches some service providers - and security practitioners - may take to help garner support and resources for their respective programs. Some of these ideas may help refine the cost factors proposed so far.

When it comes to real data, open source research efforts invariably lead to more well established and universally adopted methods used in the field of cyber security. With this note in mind, the CVSS was introduced as a possible source of real data that may be leveraged to refine the preliminary cost factors. In this same vein, other indirect remediation cost factors were introduced - and influenced - by the CVSS. The benefit would be access to large sources of real data, in addition to team familiarity with the scoring system.

OBSERVATIONS ON AUTOMATION

As noted within the Introduction and Background, the premise of the main research and development undertaken is to support the development of the ARMOUR system, whose aim is to automate computer network defence. Reference material that discusses ARMOUR suggests that this automation is intended for a military defence context, for "mission-oriented decision making". This in turn would suggest a tactical application of the ARMOUR, to thwart network-borne threats effectively and efficiently in a defence context. As offered above, patch management is lengthy and laborious, with many work elements that could be considered difficult if not impossible to automate some of the steps in the patching cycle. This may work against a rapid establishment of CoA in such a tactical context where the speed and execution of a selected CoA may be of higher importance. However, this observation may lack appropriate context and be a direct result of limited involvement in the ARMOUR project to date.

ANNEX 1 – VULNERABILITY MANAGEMENT PROCESS – DEFENCE ORGANIZATIONAL CONTEXT

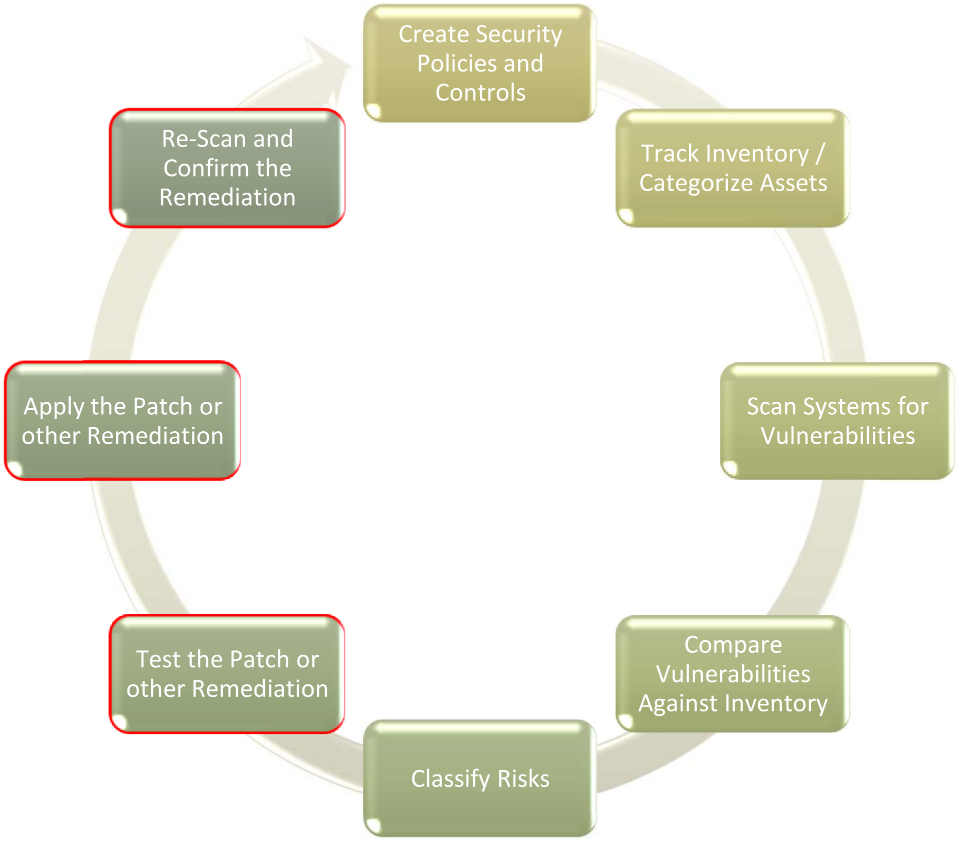

Create Security Policies and Controls
Track Inventory / Categorize Assets
Scan Systems for Vulnerabilities
Compare Vulnerabilities Against Inventory
Classify Risks
Test the Patch or other Remediation
Apply the Patch or other Remediation
Re-Scan and Confirm the Remediation

Figure 1 - Vulnerability Remediation Process

Consider the breakdown of the process above in Table 1 below with Defence Organization context provided (the red border signifies the elements of the vulnerability management process considered “remediation”). When considering the defence context in this exercise, the single most significant differentiating factor is the state of either war or peace. To emphasize the impact of the state of war on threat activities, consider the excerpt from reference [5] that describes the deliberate threat activity defined as “War”, as follows:

“Both international and civil wars or revolutions can be extremely destructive, with the potential to compromise almost every conceivable asset in every possible way. The very magnitude of war as a threat activity can complicate any associated threat assessments considerably. Therefore,

the Harmonized TRA Methodology tends to concentrate on peacetime threats and risks, even though the analytical processes are no less applicable to a wartime environment."

The significance is that defence organizations are expected to conduct war when the nation state of war is declared. This places defence organizational assets – especially those that may be deployed in theatre – at a heightened level of threat by sophisticated adversaries willing to take extreme risks.

The modern-day realities of cyber network operations (CNO) might arguably establish that nation states today are in a constant "state of war". However, experience in the cyber security field strongly suggests that the level of risk that adversary nation-states are willing to take in CNO would be considerably higher during wartime, especially in tactical warfare.

Element	Requirements	Defence Context
Create Security Policies and Controls	Policies guide security efforts for the entire organization down to configurations for security devices, servers, network services, applications and endpoints.	This can be considered a "Remediation Deployment Cost". In a defence context, these costs are usually considerable, since this often leads to the development of doctrine, policy, directives, standards, standard operating procedures, training of personnel, and material costs associated with policy enforcement and management.
Track Inventory / Categorize Assets	Vulnerabilities must be found before they can be patched. An inventory of devices, services and configurations allows correlation with known vulnerabilities for faster, accurate remediation. Categorize assets to prioritize remediation.	Defence organizations tend to be very large enterprises that account for some of the largest IT consumers in market. This results in extensive inventories of assets (software, hardware) that require significant investments in process, technology and people to track and categorize

Element	Requirements	Defence Context
		effectively.
Scan Systems for Vulnerabilities	Conduct regular or continuous scans of all devices attached to the network. Use industry standard vulnerability lists and other sources.	This differences within this element compared to a typical enterprise context would be considered negligible.
Compare Vulnerabilities Against Inventory	Identify actual vulnerabilities in the network. Minimize false positives by matching known vulnerabilities against actual configurations of devices, services and applications.	This differences within this element compared to a typical enterprise context would be considered negligible.
Classify Risks	Establish the level of risk associated with each vulnerability. This helps prioritize what to remediate first.	A standard definition for risk will have been established to consistently define and compare measured risk. In the case where a threat level (or assessment) plays a part of the defined risk level – as is the case for the GC – the types of deliberate and accidental threats will be unique within a defence context, especially in a state of war.
Test the Patch or other Remediation	Obtain the correct patch to fix the identified vulnerability and develop a remediation plan. Test patches and other remedial actions in a development environment to ensure the plan minimizes negative business impact.	This differences within this element compared to a typical enterprise context would be considered negligible. However, in the context of tactical warfare in theatre, these elements may experience accelerated

Element	Requirements	Defence Context
Apply the Patch or other Remediation	Use a patch automation system and remediation techniques that provide rollback capability in case of patch or other remediation failure.	deployment pressures, thus reducing deployment costs and presumably increasing impact costs. For example, an officer in theatre may decide to forego a testing cycle for an official fix and apply immediately, due to the perceived low-risk of impact. Similarly, in the case where a remediation solution is developed internally and unproven, a wartime scenario may force a commander to take additional risks to protect a high value asset. The likelihood of higher impact costs rises.
Re-Scan and Confirm the Remediation	Rescan to ensure the vulnerability was fixed by application of the patch or other remediation.	

Table 1 - Vulnerability Management Process Elements

ANNEX 2 – SAMPLE VULNERABILITY REMEDIATION SCENARIO

In the enterprise context – both military and non-military – vulnerability management programs are often severely tested when news of significant, wide-scope, high-profile vulnerabilities make the news. They are often high-profile because of the potential impact the vulnerability introduces: that is, exploitability is high and the results are usually catastrophic to the system or network. What often happens after the news breaks is a significant increase in broad scans across the Internet as more opportunistic threat actors attempt to find as many vulnerable systems as possible.

Let's walk through a typical scenario as introduced above:

Step 0: A high-profile vulnerability in a commonly used, broadly deployed Internet-based technology makes headlines around the world.

- **All major media outlets publish and distribute various versions of the same story.**
- **Corporate enterprises in the public, non-profit, and private sectors receive urgent requests and direction by executive managers responsible for the safety and security of their respective organizational assets.**

Step 1: A corporate enterprise impact analysis of the published vulnerability ensues. Answers are sought to questions such as:

- **Is this vulnerability relevant to our enterprise?**
- **If it is relevant, how many systems are impacted?**
- **Which systems are impacted?**
- **What are the risks to sensitive assets?**
- **Have there been any known attempts to exploit the vulnerability within our own enterprise since the public release?**

Step 2: A remediation plan to address the vulnerability is developed. Answers are sought to questions such as:

- **What is the level of effort required to address the vulnerability in its entirety? Partially?**
- **What is the impact of the plan to business operations?**
- **Who needs to approve the plan (in the case where governance is unclear)?**
- **Is the approver available to review and accept the plan?**

Step 3: The remediation plan is approved.

- **The vulnerability happens to have wide-spread impact to Internet-connected systems in the enterprise.**
- **The corporate enterprise – which is housed within a military organization – provides varying levels of security control maturity.**
- **This organization happens to have well established network security zones, with isolated network segments.**
- **The categorization of business activities and processes has ensured that assets of the highest sensitivity are logically located within the higher security zones.**

Step 4: The remediation plan is executed.

- **A communication plan is developed.**
- **The solution is tested. The test cycle time may vary based on the urgency and priority of the vulnerability impact, asset valuations, assessed threats and risks.**
- **Once successfully tested, a small subset of production systems – usually considered the highest risk systems - are placed under a scheduled and communicated outage window.**
- **The results of the remediation on the smaller subset of production systems is assessed. The end of the outage is communicated.**
- **A broader subset of production systems is placed under a scheduled and communicated outage window.**
- **The results of the remediation on the larger subset of production systems is assessed. The end of the outage is communicated.**
- **All remaining impacted production systems are placed under a scheduled and communicated outage window.**
- **The results of the remediation on the remaining subset of production systems is assessed. The end of the outage is communicated.**
- **Metrics are captured and stored for analytical and reporting purposes.**

Step 5: A Post Vulnerability Remediation Assessment takes place at the highest organizational levels. (With high-profile vulnerabilities, this appears to be a common practice since the attention garnered by the high-profile vulnerability poses an immediate danger that captures and holds the attention of the respective leadership).

- **Results associated with the remediation plan are presented to senior management and executive committees.**
- **Regular updates of the ongoing results are provided until the risks reported are mitigated to an acceptable residual.**
- **Lessons learned and a feedback exercise are performed to help improve response maturity for future high-profile vulnerabilities.**

There are many points within this scenario that can be expanded further, with additional technical detail. This common scenario should provide some foundational elements that can help extract additional relevant cost factors.

REFERENCES

[1] Solana Networks, "Preliminary Research Investigation Report - Preliminary Cost Factor List," Ottawa, 2018.

[2] N. Nakhla, K. Perrett and C. McKenzie, "Automated Computer Network Defence using ARMOUR," Defence Research and Development Canada, Ottawa, 2017.

[3] N. Schmeidler, "Calculating the Costs of Patching," 4 December 2016. [Online]. Available: http://blog.morphisec.com/cybersecurity-costs-patching. [Accessed 30 April 2018].

[4] First.Org, Inc., "Common Vulnerability Scoring System v3.0: Specification Document," FIRST.Org, Inc. (FIRST), 2017.

[5] Communications Security Estsablishment, "Harmonized Threat and Risk Assessment Methodology," Government of Canada, Ottawa, 2007.

[6] Denim Group, Ltd., "Remediation Statistics: What Does Fixing Application Vulnerabilities Cost?," RSA Conference, 2012.

[7] Qualys, Inc., "Guide to Effective Remediation of Network Vulnerabilities," Qualys, Inc., Redwood Shores, 2004.

[8] National Institute of Standards and Technology, "NIST Special Publication 800-126 Revision 3," U.S. Department of Commerce, Washington D.C., 2018.

[9] Verizon, "2018 Data Breach Investigations Report 11th Edition," Verizon, New York City, 2018.

[10] SANS Institute, "Implementing a Vulnerability Management Process," SANS Institute Reading Room, Washington D.C., 2013.

[11] European Network and Information Security Agency, "Introduction to Return on Security

Investment," European Union Agency For Network And Information Security, Heraklion, 2012.

[12] European Network and Information Security Agency, "The Cost of Incidents Affecting CIIs," European Union Agency For Network And Information Security, Heraklion, 2016.

[13] Price Waterhouse Coopers, "The Value of Vulnerability Management," Price Waterhouse Coopers, Dallas, 2006.

[14] A. Cramer, "Vulnerability Remediation – to the Cloud and Beyond!," BMC Blogs, 3 May 2017. [Online]. Available: https://www.bmc.com/blogs/tackling-vulnerability-remediation-across-multiple-platforms-bmc-secops-response-service/. [Accessed 30 April 2018].

[15] Department of Defense, "Department of Defense Manual Number 3020.45," Department of Defense, United States of America, Washington, D.C., 2008.

[16] SANS Institute InfoSec Reading Room, "Visually Assessing Possible Courses of Action for a Computer Network Incursion," SANS Institute, 2007.

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

Solana Networks
301 Moodie Drive
Suite 215 Nepean, ON K2H 9C4
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Preliminary Research Investigation Report: Remediation Cost Factors List

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Montuno, D. Y.

5. DATE OF PUBLICATION (Month and year of publication of document.)

September 2018

6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)

117

6b. NO. OF REFS (Total references cited.)

79

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada, Shirley's Bay
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

05ac - Cyber Decision making and Response (CDMR)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

W7714-115274

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2019-C029

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.) Cyber Security; Cyber Decision Making

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Remediation activities occupy a significant amount of time for network defenders. In order to effectively manage those activities, network defenders need tools and methodologies to assist them. One approach that could help network defenders in that effort is to assign cost measures to remediation activities. Determining such a cost measure is not trivial, and researchers have suggested methodologies which require knowledge of the factors that influence the cost of remediation. Unfortunately, there is no exhaustive list of such cost factors. Through a task by Defence Research and Development Canada (DRDC)'s Cyber Decision Making and Response (CDMR) project, this report documents our research efforts in determining an exhaustive list of factors that could influence remediation costs. Our sources of information are publicly available literature as well as our experiential knowledge in cyber security. We further suggest techniques that could be used to aggregate the cost factors into cost measures that could be used by defenders in prioritizing network defence activities. We further propose ways of validating those proposed measures. As recommendations for next steps, we suggest further research be carried out on algorithms that contextually aggregate relevant factors to provide dynamic and missions-relevant cost measures, which are important for applications within the Canadian Armed Forces (CAF).

Les défenseurs du réseau ont besoin d'outils et de méthodes favorisant une gestion efficace des travaux d'assainissement pour lesquels ils consacrent beaucoup de leur temps. L'attribution de mesures économiques aux travaux d'assainissement est une approche pouvant les aider à cet égard. La détermination d'une telle mesure des coûts n'est pas banale et les méthodes suggérées par les chercheurs exigent une connaissance des facteurs qui influent sur le coût de l'assainissement. Malheureusement, il n'existe pas de liste exhaustive de ces facteurs. Dans le cadre d'une tâche du projet de Prise de décision et intervention en cybernétique (PDIC) de Recherche et développement pour la défense Canada (RDDC), ce rapport précise nos efforts de recherche pour dresser une liste exhaustive des facteurs qui pourraient influencer les coûts d'assainissement. Des documents accessibles au public, ainsi que nos connaissances expérientielles en matière de cybersécurité ont servi de sources d'information. En outre, nous suggérons des techniques de regroupement des facteurs de coûts en mesure de coûts pouvant être utilisées par les défenseurs lors de la hiérarchisation des activités de défense des réseaux. Nous proposons également des moyens de valider les mesures envisagées. Pour les prochaines étapes, nous recommandons d'effectuer davantage de recherches sur les algorithmes regroupant les facteurs pertinents sur le plan contextuel pour fournir des mesures de coûts dynamiques et liées aux missions qui sont importantes au sein des Forces armées canadiennes (FAC).