****

**CISSP Risk Assessment Score by Threat and Impact Analysis -**RasbitaTM Risk management Tool

****

**Rasbita Table of contents**

| **4.1 EXECUTIVE SUMMARY .………………………………………………………………………………………….…………1**  **4.3 BUSINESS CHALLENGE .…………………………………………………………………………………………………….1**  **4.2 Business Challenge .………………………………………………………………………………………………………….1**  [**4.3 RISK ANALYSIS .…………………………………………………………………………………………………………………1**](#_heading=h.gghb29ruq0zn)  [**4.3.1 Qualitative Risk Analysis ...………………………………………………………………….………………………1**](#_heading=h.fgpcsb32sp8g)  [**4.3.2 Quantitative Risk Analysis .………………………………………………………………………………………….2**](#_heading=h.m1wg6yr5vmuz)  **4.4 SOLUTION DESCRIPTION .………………………………………………………………………………………………….2**  **4.5 BENEFITS ..………………………………………………………………………………….…………………………………….2**  **4.6 RISK RESPONSE PLANNING .………………………………………………………………………………………………2**  **4.7 TECHNICAL SPECIFICATION .………………………………………………………………………………………………3**  **4.8 TARGET MARKET .……………………………………………………………………………………………………………..3**  **4.9 CASE STUDY.……………………………………………………………………………………………………………………..3**  **5.0 SUMMARY..………………………………………………………………………………………………………………………3** |
| --- |

## 4.1 EXECUTIVE SUMMARY

CISSP- RISK ASSESSMENT SCORE BY IMPACT AND THREAT ANALYSIS. This application is to help any organization obtain the risk scores, analyze impacts and threats. The results obtained could be utilized for cost-benefit analysis deducing the Net Risk Reduction Benefit (NRRB) for the proper Actual Cost of Safeguards (ACS) needed to protect all affected assets or assets at risk. This goes a long way in helping with IT Security budgeting plus resource and risk management.

1. Risk Score

This score determines the priority given to security incidents.

1. Impact and threats

These will refer to the impact the threat has on the organization’s assets. The threat itself is that agent which puts the asset in harm’s way.

1. Annualized Loss expectancy (ALE): SLE\*ARO

This is the frequency of loss by an organization each year. Where the risk targets a specific vulnerability. This helps to determine NRRB.

1. Cost-Benefit Analysis

This will help organizations to make better decisions in allocating resources against the threat after a compromise. This also can be done before any incident to device Actual Cost of safeguards (ACS). This will help with costs associated with BCP/DRP.

**Factors on Rasbita’ Dashboard:**

1. The most frequent user to pull report
2. Most current report date and time
3. Number of Users
4. Most frequent threat
5. The least frequent threat
6. The cost of threat at minimum
7. The cost of threat at maximum
8. Highest and lowest ALE
9. Minimum and maximum Cost of safeguards (ACS)
10. Most frequent priority

## 4.2 BUSINESS CHALLENGE

The challenge is to be able to have appropriate or near accurate knowledge of a breach in order to create a decisive and cost-effective incident response approach. Same go to IT budget and resources allocation.

## 4.3 RISK ANALYSIS

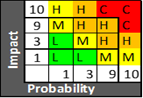
All risks identified will be assessed to identify the range of possible project outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored. Resultantly, will determine this using two (2) approaches to the analysis.

# 4.3.1 Qualitative Risk Analysis

The probability and impact of occurrence for each identified risk will be assessed by the project manager, with input from the project team using the following approach.

Probability

* Critical – Greater that <80%> probability of occurrence
* High – Between *<60%>* and <80%>probability of occurrence
* Medium – Between *<30%>* and *<60%>* probability of occurrence
* Low – Below *<30%>* probability of occurrence



Impact

* Critical - Risk that has the potential to greatly impact project cost, project schedule or performance
* High – Risk that has the potential to relatively impact project cost, project schedule or performance
* Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
* Low – Risk that has relatively little impact on cost, schedule or performance

Risks that fall within the RED, ORANGE, YELLOW and GREEN zones will have risk response planning which may include both a risk mitigation and a risk contingency plan.

# 4.3.2 Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in this section of the risk management analysis should consider:

1. *Determine the loss in value if the asset remained unprotected.*
2. *Determine the cost of protecting the asset.*
3. *Help prioritize actions and spending on security.*

**Factors in Risk Analysis used for Rasbita**

1. **Asset Value (AV)**

This refers to the asset values:

* Cost of buying/developing hardware, software and services.
* Cost of installing, maintaining upgrading hardware, software and services
* Cost to train and re-train personnel

1. **Exposure Factor (EF)**

This refers to the percentage loss that would occur from a given vulnerability being exploited by a given threat.

1. **Annualized Loss Expectancy(ALE) = ARO \* SLE**

This refers to overall loss incurred by an attack (i.e by exploiting a vulnerability) in each year.

1. **Single Loss Expectancy (SLE)** = AV \* EF

This is the most likely lost in value from an attack.

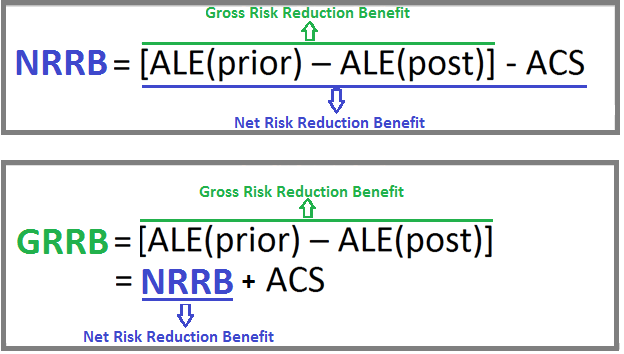
1. **Annualized Rate of Occurrence (ARO)**

This will indicate how often an attack is expected to successfully occur in a year e.g if an attack occurs once every 4 years. The ARO is .25.

1. **Annual Cost of Safeguard (ACS):** This is the cost per year of control that needs to be in place to safeguard the asset from threats.

**NRRB = [ALE(prior) – ALE(post)] – ACS**

* ALE (prior) – ALE before implementing control
* ALE (post) – ALE after implementing control
* ACS – Annual cost of Safeguard



Below is a graph of cost-benefit targeted with this Application.

***Only NRRB>0 justifies the use of safeguard/s.***

***For NRRB>=0, safeguard of up to $20000 is acceptable.***

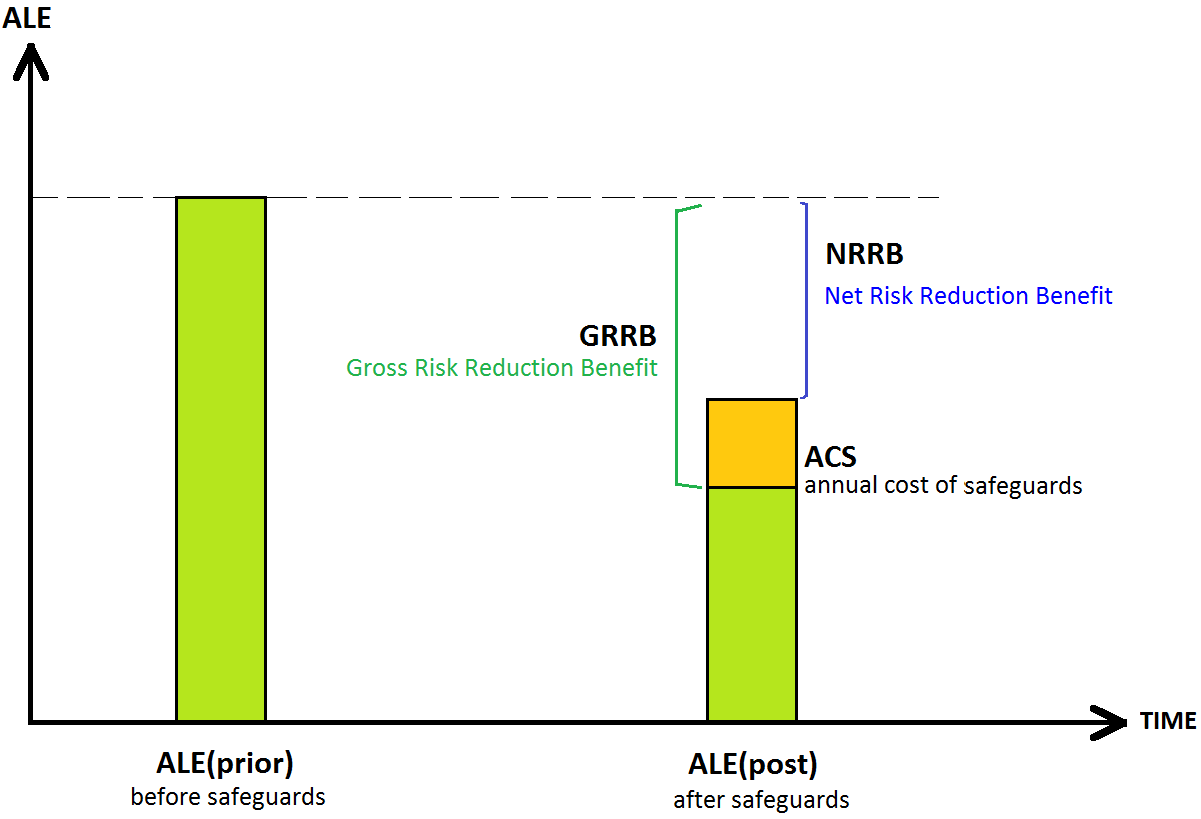


Fig 1.0 Cost – Benefit graph

The Graph below captures a cost-benefit analysis for a scenario when the safeguards put in for a specific control is 100% effective the actual cost of safeguards (ACS) even when higher: It shows that cost-benefit analysis has the lowest Net Risk Reduction Benefit (NRRB). This is a case where Annualized Loss Expectancy is pretty much ACS.

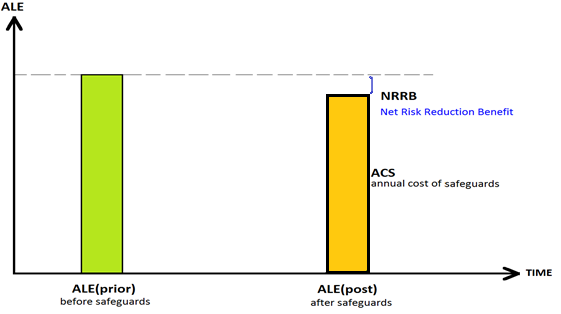


Fig 1.1 Effective safeguard graph

**4.3.2.1 Measures of Feasibility Considered in Rasbita:**

**1. Organizational Feasibility :-** This examines how well a proposed security control will contribute to an organization's strategic objectives. A firewall might be a good security safeguards, but may prevent effective flow of multimedia data-Used as example.

**2. Behavioral Feasibility :-** This examines user’s and management’s acceptance and support of a proposed security control e.g. if users do not accept a new policy/technology/ program, it will inevitably fail. DHEC must consider other measures of feasibility because one method might now work across the board in the Agency.

Most common methods for obtaining user acceptance are:

i. Communication– Affected parties must know the purpose and benefits of the proposed change.

ii. Education– Affected parties must be educated on how to work under the new constraints.

iii. Involvement– Affected parties must be given a chance to express what they want and what they will tolerate from the system.

**3. Technical Feasibility :-** This determines whether an organization has or can acquire technology and/or necessary technical expertise to implement and support a control.e.g a firewall may require a special software hardware support to be installed on all computers.

**4. Political Feasibility: -** This determines what can and cannot be done based on consensus and relationships between different departments e.g IT and IS department might have to compete for same resources.

**4.3.2.2 Relative Analysis**

It is possible for any organization to use other relative risk analyses of control in lieu of quantitative and qualitative risk analyses. Some of the measures in consideration include:

* **Benchmarking**

These will refer to study practices used in other organizations that obtain results you would like to duplicate.

* **Due Care or Due Diligence**

This is usually implementing the minimum level of security. If the minimum required or threshold is not me then the Agency could be open to legal liabilities.

* **Best Practices**

This is based on what the industry recommends. The Agency will implement an entire set of security controls as recommended for the state government. Examples of some of the best practices outlined by Microsoft are as follows:

* All computer must use antivirus
* All computers must use strong passwords
* Administrators must verify software security settings
* Update product security
* Build personal firewalls
* Back up early and often
* Protect against power surges and loses
* **Gold Standard**

This is the extra miles approach the Agency here will implement controls beyond best practices in the industry. This is fitting for an Agency striving for the best of the best in implementation of controls.

## 4.4 SOLUTION DESCRIPTION

Rasbita brings a nimble resolution to a very old problem in the IT industry regardless of the environment.

## 4.5 BENEFIT

There are tremendous benefits from the use of Rasbita as a part of first responders for IRT.

## 4.6 RISK RESPONSE PLANNING

Each major risk (those falling in the Red & Yellow zones) will be assigned to a project team member for monitoring purposes to ensure that the risk will not “fall through the cracks”.

For each major risk, one of the following approaches will be selected to address it: This could be burdensome when dealing with customer or client data.

* **Avoid** – eliminate the threat by eliminating the cause
* **Mitigate** – Identify ways to reduce the probability or the impact of the risk
* **Accept** – Nothing will be done
* **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc. For each major risk that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialize to minimize its impact.

## 4.7 TECHNICAL SPECIFICATION

**-Risk Assessment Score By Impact and Threat Analysis (RASbita)**

The assessment starts with an exercise to enumerate certain questions about devices.

Risk Score questionnaire:

1. The first question to address will be the device type whether it is a workstation, standard workstation, server or standard server. Standard will mean they have nothing like personal health record information(PHI) and Personal Identifiable Information (PII) in them.

“**Enter the device type here:”**

1. The number of devices damaged is very important as there are number of devices that will not work again after a major incident like power surge etc.,

**“Enter the number of devices damaged:”**

1. Here you will address the number of devices in the locale or department.

“**Please enter the total number of device in the locale or department:”**

1. This section will address the class of data involved in relation to the data classification at LokDon. A table is made to help users choose the right option. So we have values here in as system file =1, non-phi and pii =2, PHI =9 , PII =9

**“Enter the class of data held by the device by values shown above:”**

1. This question will address the data incident spread. What is the incident spread or coverage? The answers will have numerical values attached to them. A table is made to help users choose the right option. Widely spread = 9 and moderately spread = 5.

**“Choose the data spread or coverage shown above:”**

1. This addresses the percentage of data loss which is directly related to the infection propensity if the percentage is high the spread must have been high as well. Here we have a table showing the range required in our case.

| **The Percentage Range** | **Percentage** |
| --- | --- |
| 1-20 | 0.2 |
| 21-40 | 0.4 |
| 41-60 | 0.6 |
| 61-80 | 0.8 |
| 81-100 | 1 |

**“Please enter the percentage of data loss from the table above:”**

1. The question addresses the frequency of the business use engaged with the device mentioned in (1). Is it used on a daily basis? Is it used so often? Is it used on rare occasions? So we attached the values sample in a table: Daily basis = 9, so often = 5 and rarely used = 2.

**“Please choose the frequency of device business use as shown above:”**

1. This addresses the infrastructural environment in which the device/s is/are used. References are made to the three known environments in DHEC. Production = 9 , Staging=5 and Testing = 2. I believe workstations only have production and staging.

**“Please choose the device environment from the table above:”**

1. We need to remember the percentage we entered in (6). That way we will be choosing the right value for that percentage data loss. The table shows the necessary ranges and values**:**

| **Percentage Range** | **Values** |
| --- | --- |
| 1-20 | **10.4** |
| 21-40 | **11.8** |
| 41-60 | **13.2** |
| 61-80 | **14.6** |
| 81-100 | **16** |
|  |  |

**“Please enter the value for percentage data loss, match the percentage entered in (5):”**

**Threat Areas (dollar amount and values)**

1. This will deal with the threat values used in deriving the overall “RiskScore”. Specifically the threat weigh of the score:

| **Security incident** | **Values** |
| --- | --- |
| Denial of service/DDOS | 9 |
| Unauthorized external | 8 |
| Unauthorized internal | 9 |
| Disclosure Name and dob | 9 |
| Disclosure Name and ss | 9 |
| Social Engineering (known /unknown) | 5 |
| Malware Server | 9 |
| Malware Workstation | 9 |
| Improper usage | 5 |
| No significant loss | 0 |
|  |  |

**“Please enter the value from the table above for any given threat:”**

If the threat is more than one e.g improper use=5 and malware workstation=9 (not malware workstation is the same as standard workstation) for that device type. Please make the total value = 9.

1. This will deal with the economic or financial value used in deriving the overall “Risk management”. Our advice is to pull data from reliable sources regarding the cost of security incidents. Regular updates are needed. Specifically, the threat financial weigh or dollar amount equivalent to the score stemming from noted research works:

| **Security incident** | **$ Values** |
| --- | --- |
| Denial of service/DDOS | $30 |
| Unauthorized external | $5 |
| Unauthorized internal | $5 |
| Disclosure Name and dob | $10 |
| Disclosure Name and ss | $10 |
| Social Engineering (known /unknown) | $3 |
| Malware Server | $2160 |
| Malware Workstation | $720 |
| Improper usage | $24 |
| No significant loss | $0 |
| Disclosure Name, Dob and SS | $30 |

**“Please enter the dollar value matching the threat from the table above (10):”**

If the threat is more than one threat selection, follow question 10 indication i.e improper use=$24 and malware Workstation =$720. You must use $720 as the threat cost for workstation device types and the derivatives. If the threat is improper use = $24 and malware server = $2160. You must use **$2160**. As you can see this is showing the difference in capped financial burden between the workstation/standard workstation and server / standard server. Refer to **Limitation Added Solution #2.**

**Machine cost category**

1. This category will address the worth of each damaged workstation, server, standard workstation and server. They will be costed following the sample below:

| **Damaged Machine Category** | **$ values** |
| --- | --- |
| Damaged or lost server | $5000 |
| Damaged or lost standard server | $4000 |
| Damaged or lost workstation | $500 |
| Damaged or lost standard workstation | $300 |
| No lost applied | $0 |
|  |  |

**“Please enter the dollar value from the table above for the damaged device:”**

If you chose Workstation in (1) it means that you must choose the dollar amount corresponding to that Damaged or lost device step. If it is a workstation i.e equal to $500 too. If a user still chooses the wrong dollar amount thereby throwing an error you should catch that with an alert “Incorrect cost for <device type> try again”. In this scenario, the device type is workstation as an example.

1. Total number of data held in all the devices in the department or locale. This is supplied by the user.

**“Please enter the total number of data held in all devices in the department or locale:”**

### 4.7.1 Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in this section of the risk management analysis should consider:

1. *Determine the loss in value if the asset remained unprotected.*
2. *Determine the cost of protecting the asset.*
3. *Help prioritize actions and spending on security.*

**Factors in Risk Analysis**

1. **Asset Value (AV)**

This refers to the asset values:

* Cost of buying/developing hardware, software and services.
* Cost of installing, maintaining upgrading hardware, software and services
* Cost to train and retrain personnel

1. **Exposure Factor (EF)**

This refers to the percentage loss that would occur from a given vulnerability being exploited by a given threat.

1. **Annualized Loss Expectancy(ALE) = ARO \* SLE**

This refers to overall loss incurred by an attack (i.e by exploiting a vulnerability) in each year.

1. Single Loss Expectancy **(SLE)** = AV \* EF

This is the most likely lost in value from an attack.

1. **Annualized Rate of Occurrence (ARO)**

This will indicate how often an attack is expected to successfully occur in a year e.g if an attack occurs once every 4 years. The ARO is .25.

**EF** = dataPercent -> percentage of the damage spread when threat targets a specific vulnerability

**AV** = (damCost\* numDevices) +( addCalc(totnum\_asset, dataPercent) \*threatCost)

**SLE** = (damCost\* numDevices) +( addCalc(totnum\_asset, dataPercent) \*threatCost) \* dataPercent

**ARO** = How often do you think this kind of attack will happen in a year? The user will have to supply this. E.g 1s in a year enter 1: 1s in 2 years enter .5: 1s in four years enter .25. etc.,

**ALE** = ARO \* (damCost\* numDevices) +( addCalc(totnum\_asset, dataPercent) \*threatCost) \* dataPercent

From above you can see that it is possible to present a table like the above to the user reflecting the impact of the threat which exploited a specific vulnerability. Questions will commence henceforth

1. Annualized Rate of Occurrence: How often an attack will happen in a year.

Occurrence/number of years

**“Enter your Annualized Rate of Occurrence (ARO) for the security incident:”**

* Once /year = 1
* Once /2yr = .5
* Once /3yr = .33
* Once/4yr = .25

With this ARO you can fill out the values in the table above easily.

**<Company> USE OF ARO, SLE TO DETERMINE ALE**

| **Asset** | **Risk/Vuln** | **Asset Value $** | **Exposure Factor(EF)** | **SLE=AV\*EF**  **$** | **Annualize Freq (ARO)** | **ALE**  **$** |
| --- | --- | --- | --- | --- | --- | --- |
| Client Data(PII) | hacked | 14,000000 | .6 | 8400000 | .25 | 2100000 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. Risk Score

This score determines the priority given to security incidents.

1. Impact and threats

These will refer to the impact the threat has on the organization’s assets. The threat itself is that agent which puts the asset in harm’s way.

1. Annualized Loss expectancy (ALE): SLE\*ARO

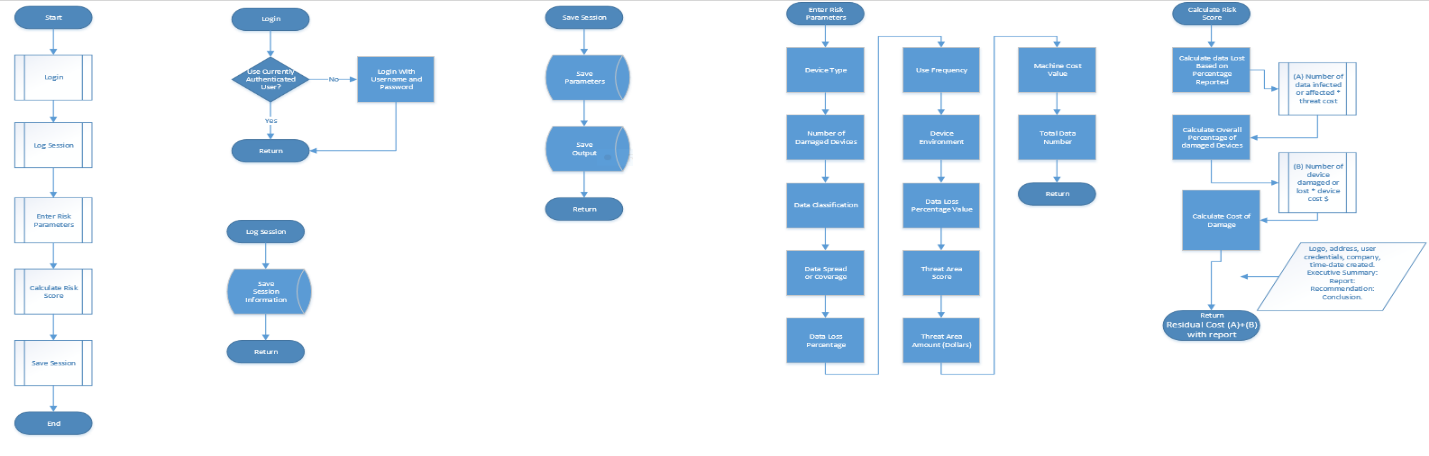
This is the frequency of loss by an organization each year. Where the risk targets a specific vulnerability. This helps to determine NRRB.

1. Cost-Benefit Analysis

This will help organizations to make better decisions in allocating resources against the threat after a compromise. This also can be done before any incident to device Actual Cost of safeguards (ACS). This will help with costs associated with BCP/DRP.

**Conclusion:**

The risk score is a part of risk management. This tool answers the question of quantifying the damages and the infections to monetary value. These pieces of information are vital in a dynamic threat-scape. The CISO, other executives and stakeholders need to know right away the cost of any event whether it is a security incident or not. This need to know in a timely manner spurns the Risk Score tool. We can now cover and report the threat cost and overall damages after any attack in the IT environment. We can equally apply this to other program area with a little customization.



## 4.8 TARGET MARKET

The target

## 4.9 CASE STUDY

Use Case Scenario:

A typical example to use will be the SC breach of 2012. There was a massive breach of 3.6M social security numbers and credit card numbers. More so, 387, 000 credit and debit cards belonging to taxpayers.- We will just pay attention to the 3.6M. This was the result of an IRS server compromise by international hackers. It cost the state about 2 dollars for each social security number. More so, it is possible that if there are no appropriate controls in place these security breaches could repeat every 5 years. Rasbita can use this case to derive a cost-benefit analysis.

**Rasbita USE OF ARO, SLE TO DETERMINE ALE**

| **Asset** | **Risk/Vulnerability** | **Asset Value $** | **Exposure Factor(EF)** | **SLE=AV\*EF**  **$** | **Annualize Freq (ARO)** | **ALE**  **$** |
| --- | --- | --- | --- | --- | --- | --- |
| Data Base(PII) | Unauthorized External (hacked) | 7200000 | .8 | 5760000 | .20 | **1152000** |
|  |  |  |  |  |  |  |

**Cost Benefit Analysis:** This expresses the cost benefit of a safeguard. Particularly, this determines whether a control is worth its cost. Simply put this determines whether a security control measure is feasible economically. From above the ***ACS < $1152000*** will be satisfactory.

## 5.0 SUMMARY

Rasbita should be retained as a part of the sleuth of risk management tools. This tool answers the question of quantifying the damages and the infections to monetary value. These pieces of information are vital in a dynamic threat-scape. The CISO, other executives and stakeholders need to know right away the cost of any event whether it is a security incident or not. This need to know in a timely manner spurns the risk score assessment by impact and threat analysis represented in a simple application or software. We can now cover and report the threat cost and overall damages after any attack in the IT environment. We can equally apply this in many program areas with a little customization.

**Definition**

**Appendix**

