**OPISPA-V Case Study,**

|  |
| --- |
| Info 1: OPISPA-V is a tool, which calculates and visualizes distribution of risks and costs to the threats and selected precautions in an optimum manner. Figure 1 shows the main menu structure and the flow of actions. |

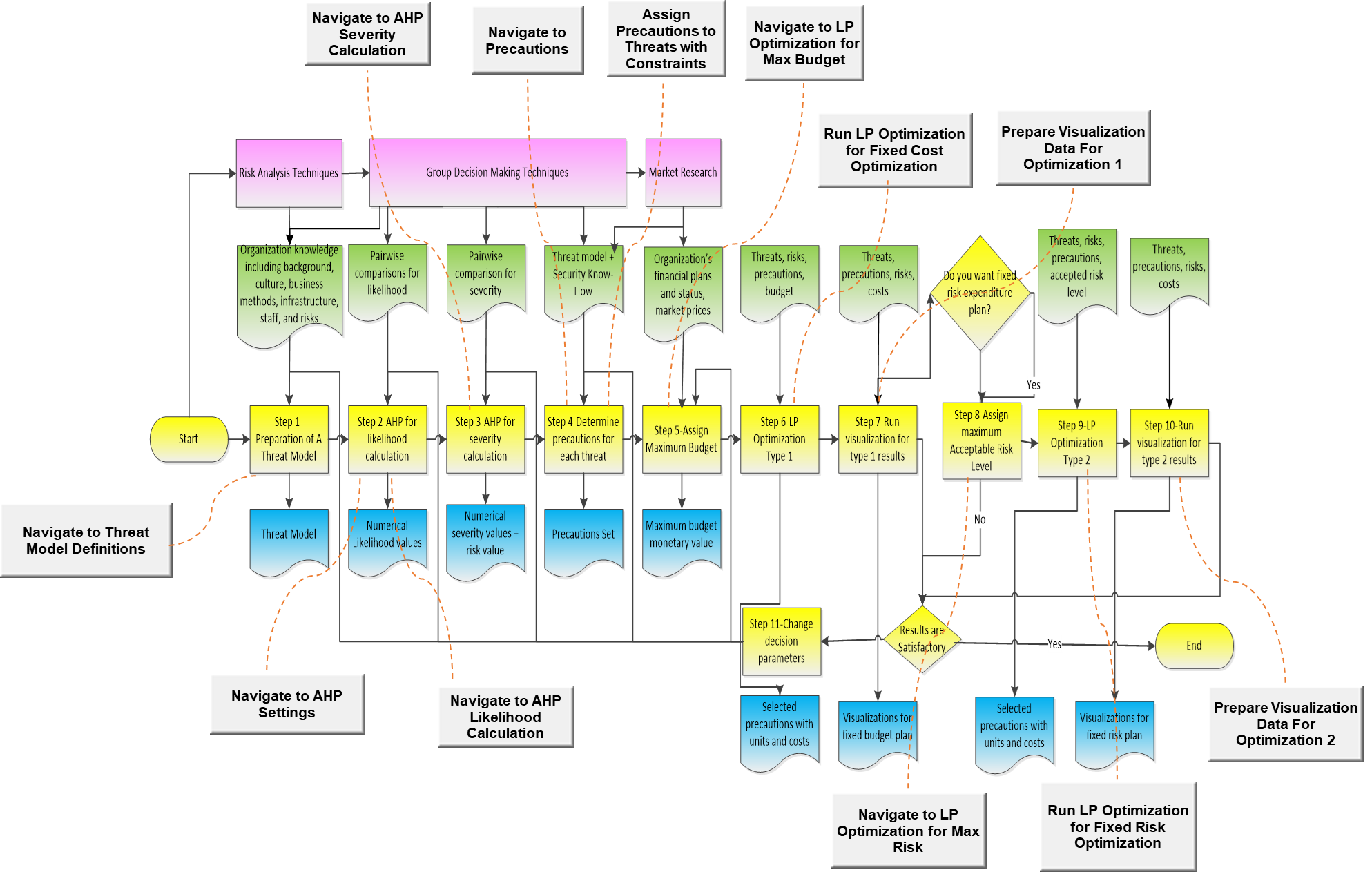
****

Figure 1

|  |
| --- |
| Step 1: A threat model for the selected organization should be prepared. This may be the result of some formal or informal approaches such that group decision making, risk analysis methods, vulnerability scanners, and experts evaluation techniques.  Inputs: Organization knowledge including background, culture, business methods, infrastructure, staff, and risks specific to that organization.  Output: A threat model which include names of threats in a grouped manner. |

|  |
| --- |
| Question 1: Do you examine threats in detail and build a threat model when you determining a budget for the security installation or improvement expenditure for your organization?  Yes …………. No ………….. |

Table 1-Threat Model

|  |  |  |  |
| --- | --- | --- | --- |
| Threats to The Level of Service | Power Loss | Power Loss | T1 |
| Hardware Failure | Hardware Failure | T2 |
| Software Crash | Software Crash | T3 |
| System Operators | Operator Errors | T4 |
| Authorized Users |
| Programmers |
| The Rest of The World |
|  | Malicious Inside Action | T5 |
| Viruses | Trojan and Worms | T6 |
| Trojan |
| Worms |
|  | Fire | T7 |
| Explosions | Other Environmental Disasters | T8 |
| Floods |
| Earthquakes |
|  | Availability Threats(DDOS) | T9 |
| Threats to the Information Base |  | Disk Failure | T10 |
|  | Data Corruption | T11 |
|  | Inaccurrate Data | T12 |
| Covert Channel | Un-authorized Access | T13 |
| Mandatory Access Control |
| Discretionary Access Control |
| Physical Access Control |
|  | Virus and Spyware | T14 |
| Threats to Information Leakage | Hacking | Hacking | T15 |
| Keylogger |
| Backdoor |
| Media Leakage | Media Leakage | T16 |
| Theft of Media |
| Tempest |
| Botnet | Communication Preventers(Botnet, Dialer) | T17 |
| Dialer |
|  | Authentication Threats | T18 |
|  | Non Repudiation Threats | T19 |
|  | Separation of Duties | T20 |
|  | Configuration Threats | T21 |
|  | Communications Threats | T22 |

|  |
| --- |
| Question 2: Do you think dividing and analyzing the threats into multiple groups, such as “Threats to The Level of Service”, “Threats to the Information Base”, and “Threats to Information Leakage” is advantageous compared to examining all threats in one group?  Yes …………. No ………….. |

|  |
| --- |
| Step 2: Pairwise comparison of likelihood of threats to assign numerical likelihood values for each.  Input: Comparison matrix for likelihood  Output: Numerical likelihood values |

Inputs for Likelihood Pairwise Comparisons:

|  |  |  |  |
| --- | --- | --- | --- |
| Thread Groups | Threats to The Level of Service | Threats to the Information Base | Threats to Information Leakage |
| Threats to The Level of Service | 1 | 1/3 | 1/5 |
| Threats to the Information Base | 3 | 1 | 1 |
| Threats to Information Leakage | 5 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1-Power Loss | T2-Hardware Failure | T3-Software Crash | T4-Operator Errors | T5-Malicious Inside Action | T6-Trojan and Worms | T7-Fire | T8-Other Environmental Disasters | T9-Availability Threats(DDOS) |
| T1-Power Loss | 1 | 6 | 6 | 6 | 9 | 8 | 9 | 9 | 9 |
| T2-Hardware Failure | 1/6 | 1 | 1/2 | 1/4 | 1/6 | 1/6 | 2 | 2 | 1 |
| T3-Software Crash | 1/6 | 2 | 1 | 6 | 3 | 1/4 | 5 | 6 | 6 |
| T4-Operator Errors | 1/6 | 4 | 1/6 | 1 | 4 | 1 | 6 | 6 | 2 |
| T5-Malicious Inside Action | 1/9 | 6 | 1/3 | 1/4 | 1 | 1/3 | 3 | 3 | 1 |
| T6-Trojan and Worms | 1/8 | 6 | 4 | 1 | 3 | 1 | 8 | 8 | 5 |
| T7-Fire | 1/9 | 1/2 | 1/5 | 1/6 | 1/3 | 1/8 | 1 | 2 | 1 |
| T8-Other Enviromental Disasters | 1/9 | 1/2 | 1/6 | 1/6 | 1/3 | 1/8 | 1/2 | 1 | 1/3 |
| T9-Availability Threats(DDOS) | 1/9 | 1 | 1/6 | 1/2 | 1 | 1/5 | 1 | 3 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T10-Disk Failure | T11-Data Corruption | T12-Inaccurrate Data | T13-Un-authorized Access | T14-Virus and Spyware |
| T10-Disk Failure | 1 | 1/2 | 1 | 1/4 | 1/6 |
| T11-Data Corruption | 2 | 1 | 1 | 1/5 | 1/7 |
| T12-Inaccurrate Data | 1 | 1 | 1 | 1/5 | 1/8 |
| T13-Un-authorized Access | 4 | 5 | 5 | 1 | 1/9 |
| T14-Virus and Spyware | 6 | 7 | 8 | 9 | 1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T15-Hacking | T16-Media Leakage | T17-Communication Preventers(Botnet, Dialer) | T18-Authentication Threats | T19-Non Repudiation Threats | T20-Separation of Duties | T21-Configuration Threats | T22- Communications Threats |
| T15-Hacking | 1 | 2 | 1/3 | 1/5 | 1/5 | 1/3 | 1/3 | 1/4 |
| T16-Media Leakage | 1/2 | 1 | 1/5 | 1/6 | 1/6 | 1/6 | 1/6 | 1/5 |
| T17-Communication Preventers(Botnet, Dialer) | 3 | 5 | 1 | 1/2 | 1 | 1 | 1/2 | 1 |
| T18-Authentication Threats | 5 | 6 | 2 | 1 | 2 | 2 | 3 | 2 |
| T19-Non Repudiation Threats | 5 | 6 | 1 | 1/2 | 1 | 1 | 1/2 | 1/2 |
| T20-Separation of Duties | 3 | 6 | 1 | 1/2 | 1 | 1 | 1 | 2 |
| T21-Configuration Threats | 3 | 6 | 2 | 1/3 | 2 | 1 | 1 | 2 |
| T22- Communications Threats | 4 | 5 | 1 | 1/2 | 2 | 1/2 | 1/2 | 1 |

Likelihood Results:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | **Threat Name** | **Threat Likelihood** | # | **Threat Name** | **Threat Likelihood** |
| 1 | T14-Virus and Spyware | 0.706364366 | 12 | T11-Data Corruption | 0.09379517 |
| 2 | T18-Authentication Threats | 0.581845632 | 13 | T3-Software Crash | 0.089952409 |
| 3 | T21-Configuration Threats | 0.38319827 | 14 | T12-Inaccurrate Data | 0.073606513 |
| 4 | T20-Separation of Duties | 0.331721413 | 15 | T10-Disk Failure | 0.072917933 |
| 5 | T22- Communications Threats | 0.293154023 | 16 | T4-Operator Errors | 0.067227327 |
| 6 | T19-Non Repudiation Threats | 0.286433822 | 17 | T16-Media Leakage | 0.058604824 |
| 7 | T17-Communication Preventers(Botnet, Dialer) | 0.271243237 | 18 | T5-Malicious Inside Action | 0.044492643 |
| 8 | T13-Un-authorized Access | 0.269766233 | 19 | T9-Availability Threats(DDOS) | 0.023550794 |
| 9 | T1-Power Loss | 0.242949824 | 20 | T2-Hardware Failure | 0.023492987 |
| 10 | T6-Trojan and Worms | 0.104077572 | 21 | T7-Fire | 0.016665052 |
| 11 | T15-Hacking | 0.095674682 | 22 | T8-Other Environmental Disasters | 0.01203952 |

|  |
| --- |
| Step 3: Pairwise comparison of threats to assign numerical severity values for each.  Input: Comparison matrix for severity  Output: Numerical severity values |

Inputs for Severity Pairwise Comparisons:

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Groups | Threats to The Level of Service | Threats to the Information Base | Threats to Information Leakage |
| Threats to The Level of Service | 1 | 4 | 3 |
| Threats to the Information Base | 1/4 | 1 | 1 |
| Threats to Information Leakage | 1/3 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Threat Names | T1-Power Loss | T2-Hardware Failure | T3-Software Crash | T4-Operator Errors | T5-Malicious Inside Action | T6-Trojan and Worms | T7-Fire | T8-Other Environmental Disasters | T9-Availability Threats(DDOS) |
| T1-Power Loss | 1 | 1/9 | 1/9 | 1/9 | 1/9 | 1/9 | 1/9 | 1/9 | 1/9 |
| T2-Hardware Failure | 9 | 1 | 4 | 3 | 1 | 3 | 1/7 | 1/7 | 1/3 |
| T3-Software Crash | 9 | 1/4 | 1 | 1/3 | 1/4 | 1/6 | 1/9 | 1/9 | 1/5 |
| T4-Operator Errors | 9 | 1/3 | 3 | 1 | 1/3 | 1/2 | 1/8 | 1/8 | 1/4 |
| T5-Malicious Inside Action | 9 | 1 | 4 | 3 | 1 | 6 | 1 | 1 | 4 |
| T6-Trojan and Worms | 9 | 1/3 | 6 | 2 | 1/6 | 1 | 1/8 | 1/9 | 1/3 |
| T7-Fire | 9 | 7 | 9 | 8 | 1 | 8 | 1 | 1 | 7 |
| T8-Other Environmental Disasters | 9 | 7 | 9 | 8 | 1 | 9 | 1 | 1 | 7 |
| T9-Availability Threats(DDOS) | 9 | 3 | 5 | 4 | 1/4 | 3 | 1/7 | 1/7 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T10-Disk Failure | T11-Data Corruption | T12-Inaccurrate Data | T13-Un-authorized Access | T14-Virus and Spyware |
| T10-Disk Failure | 1 | 1/3 | 5 | 1/4 | 3 |
| T11-Data Corruption | 3 | 1 | 1 | 1/3 | 1 |
| T12-Inaccurrate Data | 1/5 | 1 | 1 | 1/4 | 1/3 |
| T13-Un-authorized Access | 4 | 3 | 4 | 1 | 1/3 |
| T14-Virus and Spyware | 1/3 | 1 | 3 | 3 | 1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T15-Hacking | T16-Media Leakage | T17-Communication Preventers(Botnet, Dialer) | T18-Authentication Threats | T19-Non Repudiation Threats | T20-Separation of Duties | T21-Configuration Threats | T22- Communications Threats |
| T15-Hacking | 1 | 8 | 4 | 4 | 4 | 6 | 6 | 3 |
| T16-Media Leakage | 1/8 | 1 | 1/3 | 1/4 | 1/4 | 1/3 | 1/3 | 1/4 |
| T17-Communication Preventers(Botnet, Dialer) | 1/4 | 3 | 1 | 1 | 1 | 3 | 1 | 1 |
| T18-Authentication Threats | 1/4 | 4 | 1 | 1 | 1 | 2 | 2 | 1 |
| T19-Non Repudiation Threats | 1/4 | 4 | 1 | 1 | 1 | 2 | 1 | 1 |
| T20-Separation of Duties | 1/6 | 3 | 1/3 | 1/2 | 1/2 | 1 | 1/4 | 1/6 |
| T21-Configuration Threats | 1/6 | 3 | 1 | 1/2 | 1 | 4 | 1 | 1 |
| T22- Communications Threats | 1/3 | 4 | 1 | 1 | 1 | 6 | 1 | 1 |

Severity Results:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Threat Names** | **Threat Severity** | **#** | **Threat Names** | **Threat Severity** |
| 1 | T8-Other Environmental Disasters | 0.884864571 | 12 | T10-Disk Failure | 0.116253072 |
| 2 | T7-Fire | 0.872529401 | 13 | T3-Software Crash | 0.11194896 |
| 3 | T5-Malicious Inside Action | 0.539469801 | 14 | T18-Authentication Threats | 0.104559494 |
| 4 | T15-Hacking | 0.345902913 | 15 | T17-Communication Preventers(Botnet, Dialer) | 0.096281665 |
| 5 | T9-Availability Threats(DDOS) | 0.30468506 | 16 | T19-Non Repudiation Threats | 0.095385566 |
| 6 | T2-Hardware Failure | 0.287841266 | 17 | T21-Configuration Threats | 0.09100092 |
| 7 | T6-Trojan and Worms | 0.189186761 | 18 | T11-Data Corruption | 0.086691317 |
| 8 | T13-Un-authorized Access | 0.15672516 | 19 | T20-Separation of Duties | 0.044577544 |
| 9 | T4-Operator Errors | 0.154645455 | 20 | T1-Power Loss | 0.043966706 |
| 10 | T14-Virus and Spyware | 0.126776335 | 21 | T12-Inaccurrate Data | 0.038115521 |
| 11 | T22- Communications Threats | 0.118146645 | 22 | T16-Media Leakage | 0.027654024 |

Overall AHP Results:

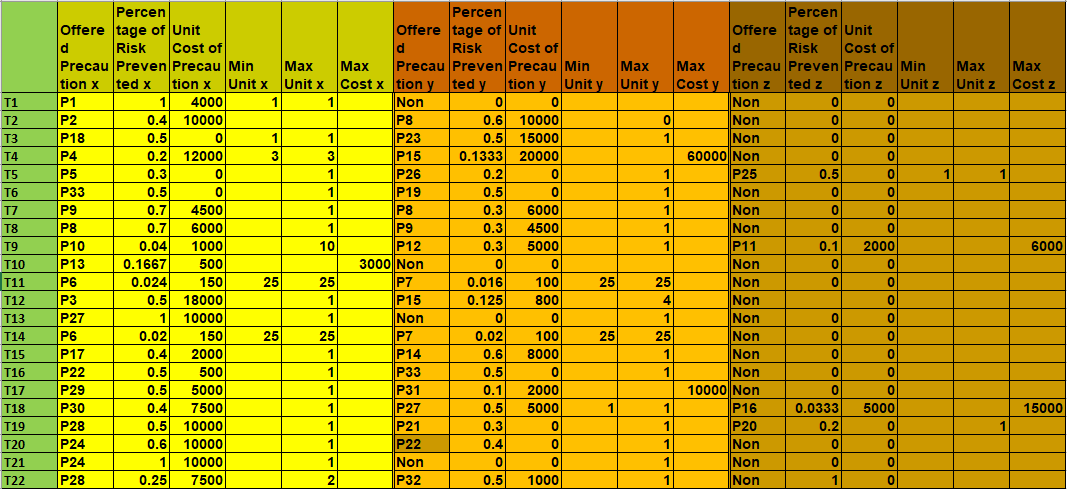
|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Names** | **Threat Severity** | **Threat Likelihood** | **Risk** |
| T14-Virus and Spyware | 0.126776335 | 0.706364366 | 0.08955 |
| T18-Authentication Threats | 0.104559494 | 0.581845632 | 0.060837 |
| T13-Un-authorized Access | 0.15672516 | 0.269766233 | 0.042279 |
| T21-Configuration Threats | 0.09100092 | 0.38319827 | 0.034871 |
| T22- Communications Threats | 0.118146645 | 0.293154023 | 0.034635 |
| T15-Hacking | 0.345902913 | 0.095674682 | 0.033094 |
| T19-Non Repudiation Threats | 0.095385566 | 0.286433822 | 0.027322 |
| T17-Communication Preventers(Botnet, Dialer) | 0.096281665 | 0.271243237 | 0.026116 |
| T05-Malicious Inside Action | 0.539469801 | 0.044492643 | 0.024002 |
| T06-Trojan and Worms | 0.189186761 | 0.104077572 | 0.01969 |
| T20-Separation of Duties | 0.044577544 | 0.331721413 | 0.014787 |
| T07-Fire | 0.872529401 | 0.016665052 | 0.014541 |
| T01-Power Loss | 0.043966706 | 0.242949824 | 0.010682 |
| T08-Other Environmental Disasters | 0.884864571 | 0.01203952 | 0.010653 |
| T04-Operator Errors | 0.154645455 | 0.067227327 | 0.010396 |
| T03-Software Crash | 0.11194896 | 0.089952409 | 0.01007 |
| T10-Disk Failure | 0.116253072 | 0.072917933 | 0.008477 |
| T11-Data Corruption | 0.086691317 | 0.09379517 | 0.008131 |
| T09-Availability Threats(DDOS) | 0.30468506 | 0.023550794 | 0.007176 |
| T02-Hardware Failure | 0.287841266 | 0.023492987 | 0.006762 |
| T12-Inaccurrate Data | 0.038115521 | 0.073606513 | 0.002806 |
| T16-Media Leakage | 0.027654024 | 0.058604824 | 0.001621 |

|  |
| --- |
| Step 4: Find out proper precautions for each threat. You may offer up to three precaution for each threat such that each will have a percentage of risk diminish factor with a total of %100 of risk diminishing for a threat. Define constraints for budget allocation. How many of each precaution item do you need? Do you have upper and lower limits for this units? Do you have any upper limit for a specific item budget such that spending at most xx much of amount to some precaution. At this step the deciders should have to make a market research and technical analyses to decide on this constraints.  Input: Threats, security know-how  Output: Precaution set |

Precaution List:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Description** | **Name** | **Description** | **Name** | **Description** |
| P1 | Install UPS | P12 | Traffic Management | P23 | Service level software agreement, PAAS |
| P2 | Replicate Servers | P13 | Backup Tapes | P24 | Auditing |
| P3 | Add validation to forms in enterprise software | P14 | Firewall | P25 | Pre-employment screening |
| P4 | Education and Assessment of Security Personal | P15 | Improvement in Data Distribution and Data Governance Policies | P26 | Mandatory vacations |
|  |  |  |  |  |  |
| P5 | Functional Isolation | P16 | Pretty Good Privacy | P27 | Identity and Access Management (IAM) Systems |
| P6 | Anti-Virus | P17 | Strong passwords | P28 | Encryption Solutions |
| P7 | Anti-Spam | P18 | Regular software patches | P29 | Intrusion Detection and Prevention Systems |
| P8 | Disaster Recovery Center on Cloud Systems | P19 | Use of 64 bit OS | P30 | Digital Signatures |
| P9 | FHM System | P20 | Turnoff Auto-Run | P31 | Trusted Communication Channels |
| P10 | Increasing bandwidth | P21 | Load – Un-Load Drivers | P32 | Integrity Check |
| P11 | Bandwidth throttling techniques | P22 | Increase Physical Security | P33 | Limit Transfer of Executables |

Precaution Cost and Constraints:



|  |
| --- |
| Step 5: Assign a maximum budget for security costs for this expenditure plan.  Inputs: Organization’s financial plans and status, market prices.  Outputs: Maximum budget monetary value. |

|  |
| --- |
| Info 2: At this step the user may run the model for various amounts of budgets. For demonstration purposes OPISPA-V LP Optimization 1 is executed for 100000, 60000, and 30000 amount of budget for the same threats using the same precautions and constraints. |

Maximum Budget for Sample Case1 = 100000

Maximum Budget for Sample Case2 = 60000

Maximum Budget for Sample Case3 = 30000

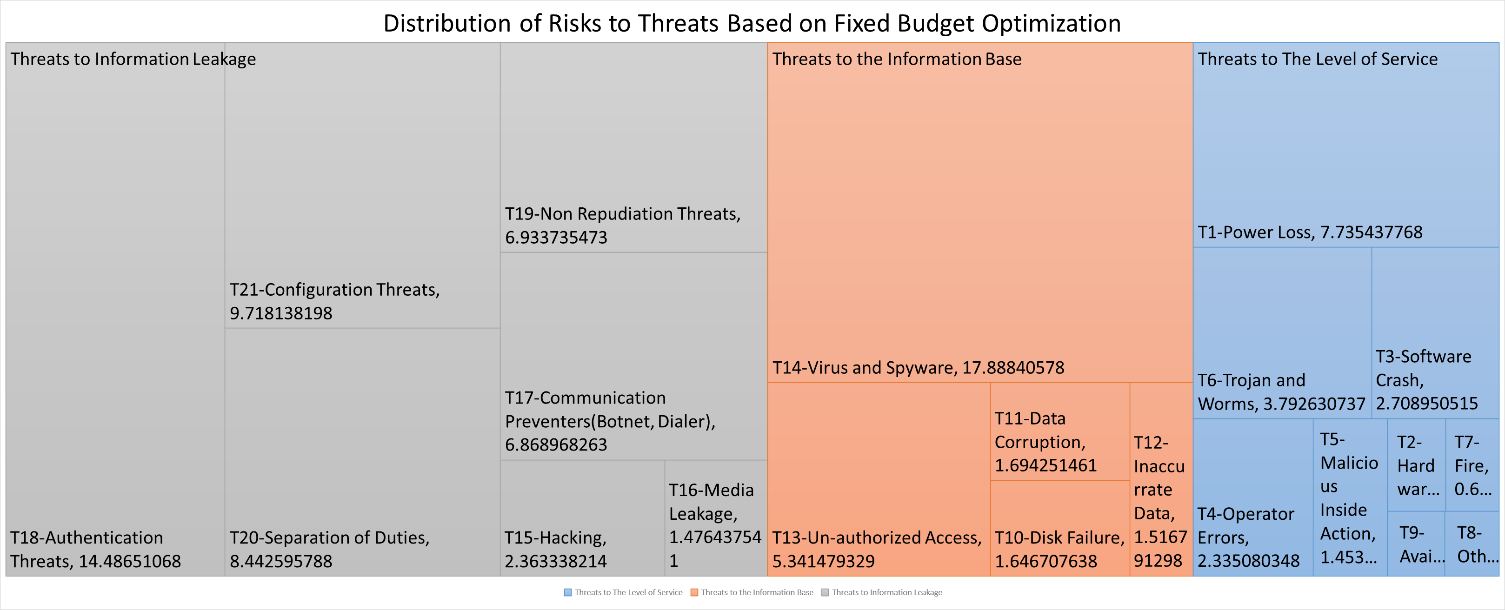
|  |
| --- |
| Step 6: Run optimization type 1 to determine best precaution choices for the fixed budget option.  Inputs: Threats, risks, precautions, budget  Outputs: Selected precautions with units and costs |

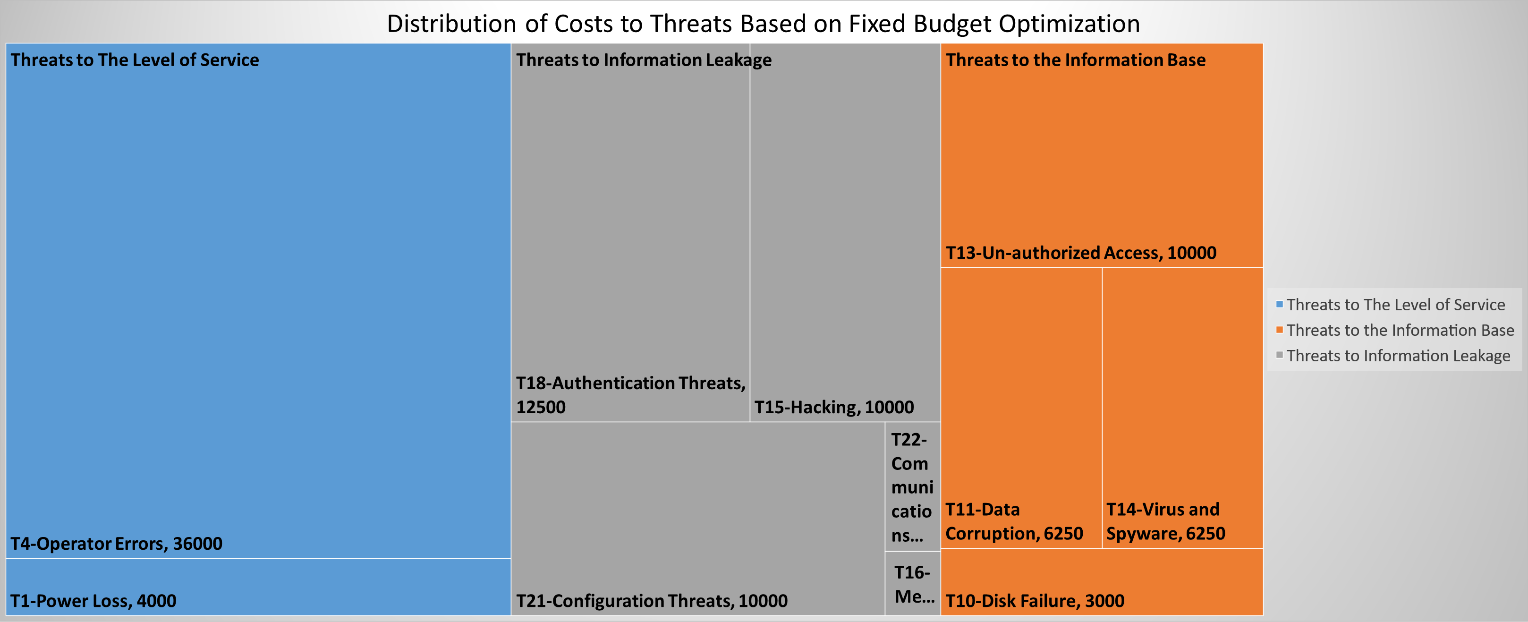
\*\*\*30000 amount of budget did not find a solution due to constraints

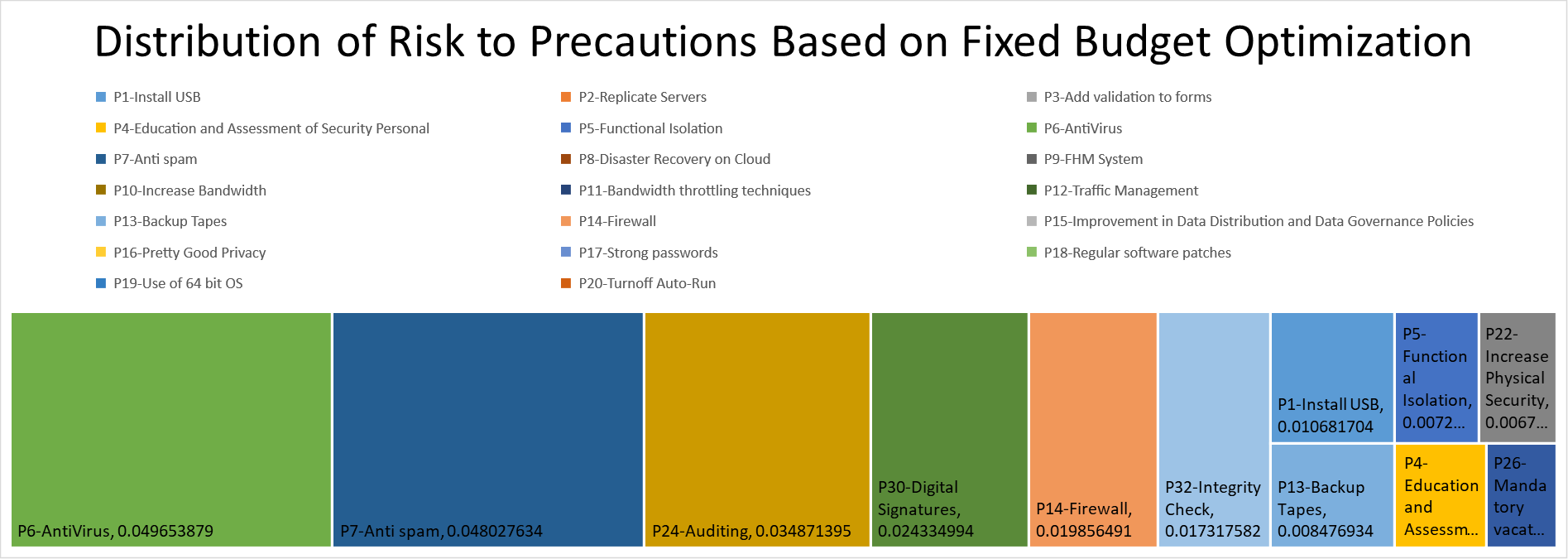
|  |  |  |
| --- | --- | --- |
|  | For 100000 budget | For 60000 budget |
| Budget Spent | 99500 | 60000 |
| Number of Threats Handled | 16 | 13 |
| Eliminated Risks(Tx) | T1,T3,T4,T5,T6,T9, T10,T11, T13, T14, T15, T16, T18, T19, T20, T22 | T1,T3,T4,T5,T6,T10,T11,T14,T16,T18,T19,T20, T22 |
| Percentage of Eliminated Risk over Total Risk | %75.29 | %47.28 |
| Selected Pecautions by Optimization(Px(unit)) | P1(1), P4(3), P5(1), P6(50), P7(50), P13(6), P14(1), P17(1), P18(1),  P19(1), P20(1), P21(1),  P22(1), P24(1), P25(1), P26(1),  P27(2), P30(1), P32(1),  P33(2) | P1(1), P4(3), P5(1), P6(50), P7(50), P13(3),  P18(1), P19(1), P20(1), P21(1), P22(1),  P25(1), P26(1), P27(1), P32(1), P33(2) |

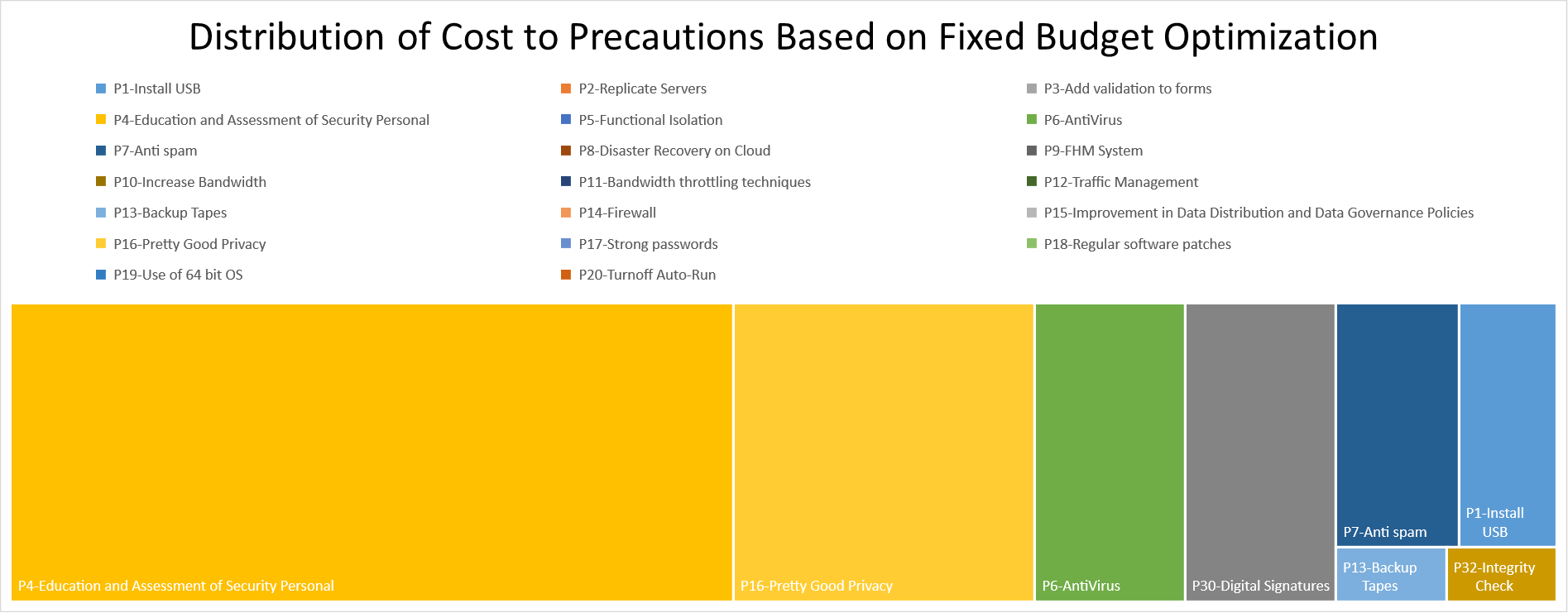
|  |
| --- |
| Step 7: Run visualization for type 1 results to examine the distribution in fixed budget option.  Inputs: Threats, risks, precautions, costs, units  Outputs: Visualizations |

Visualizations for 100000 Budget:

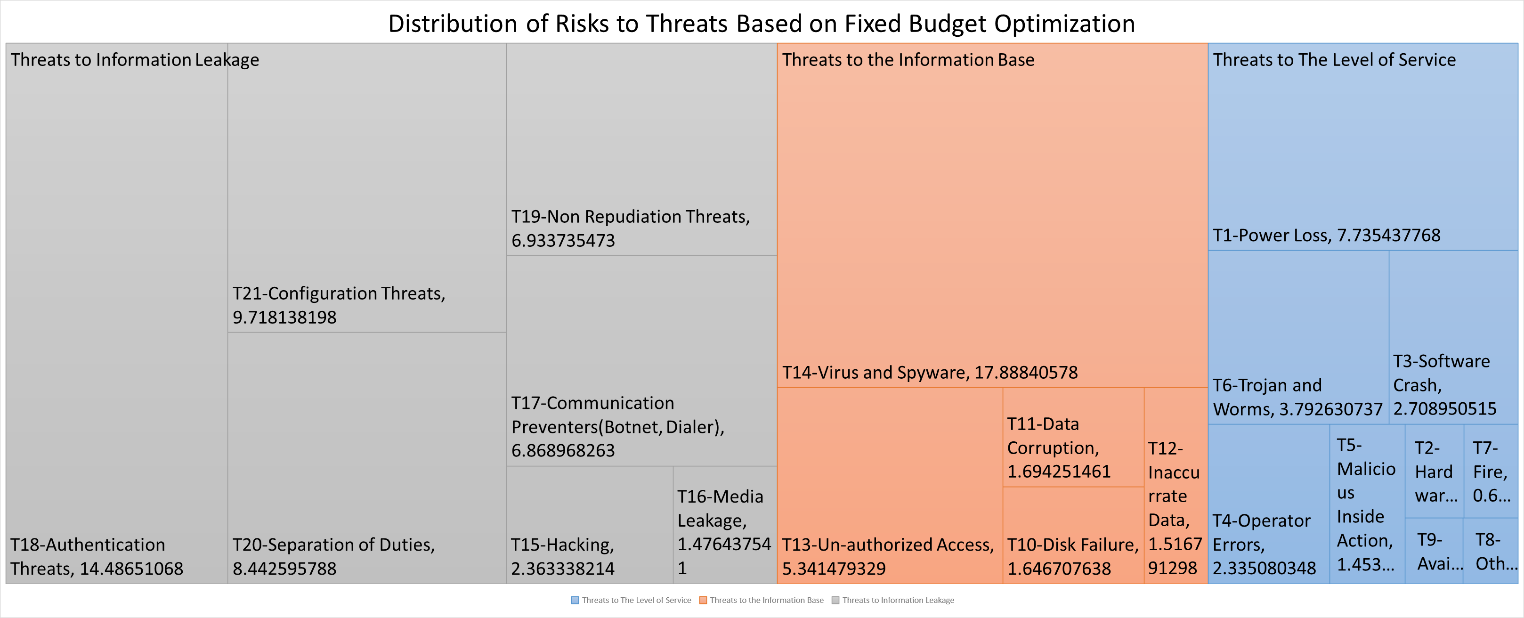


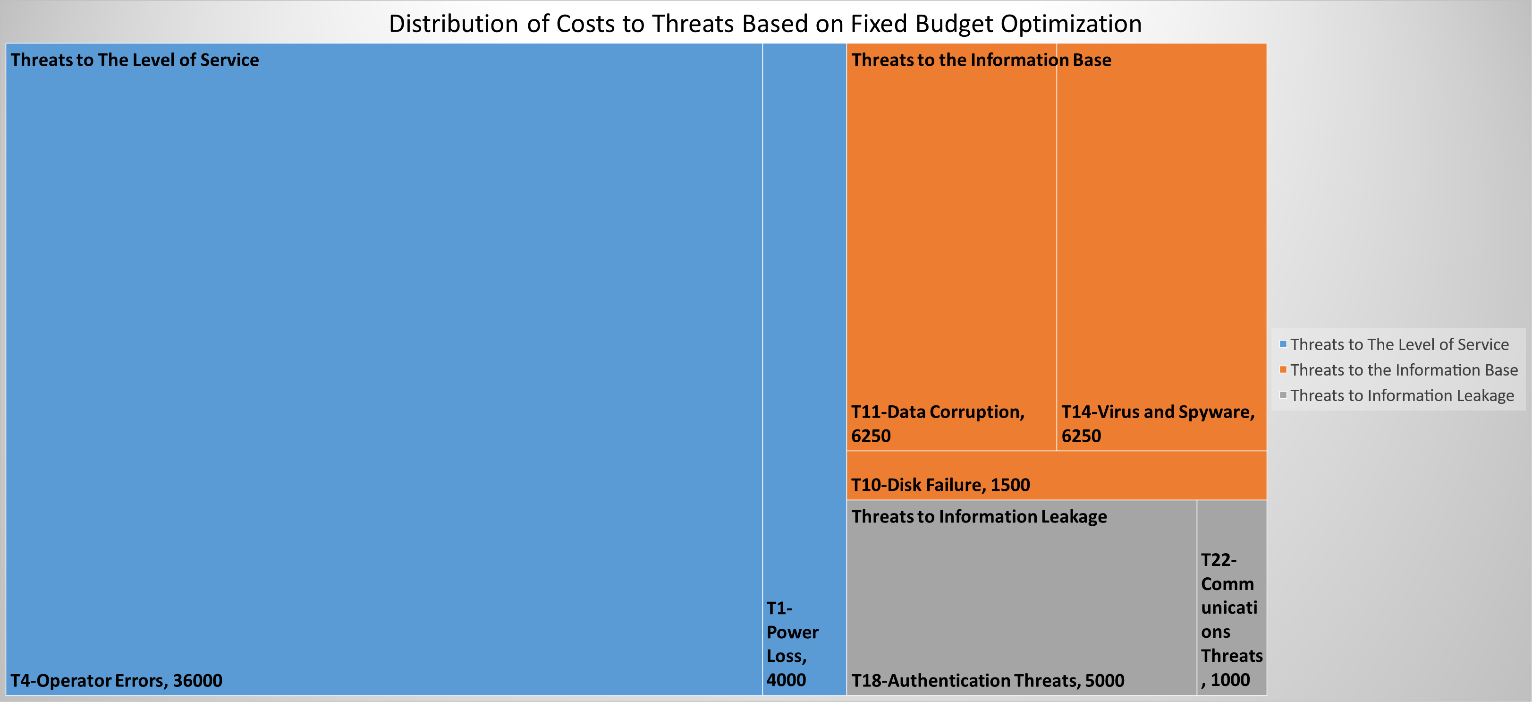


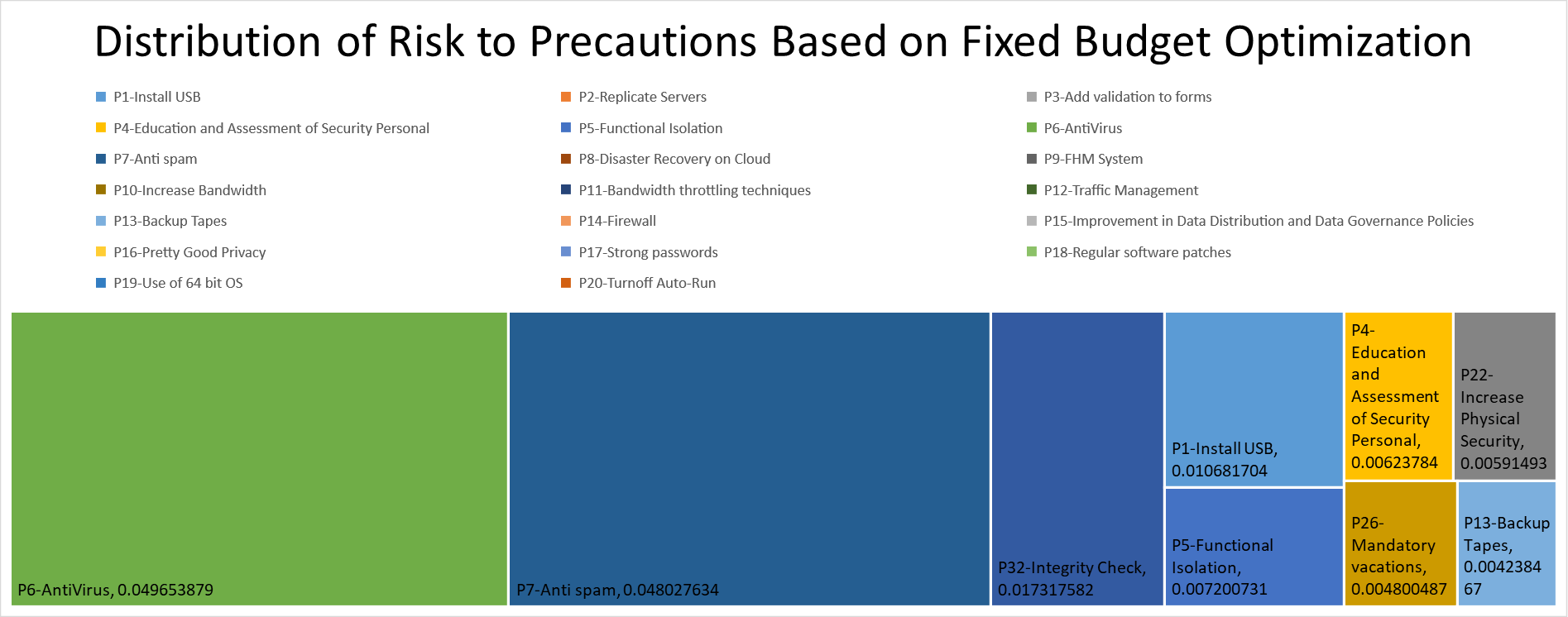


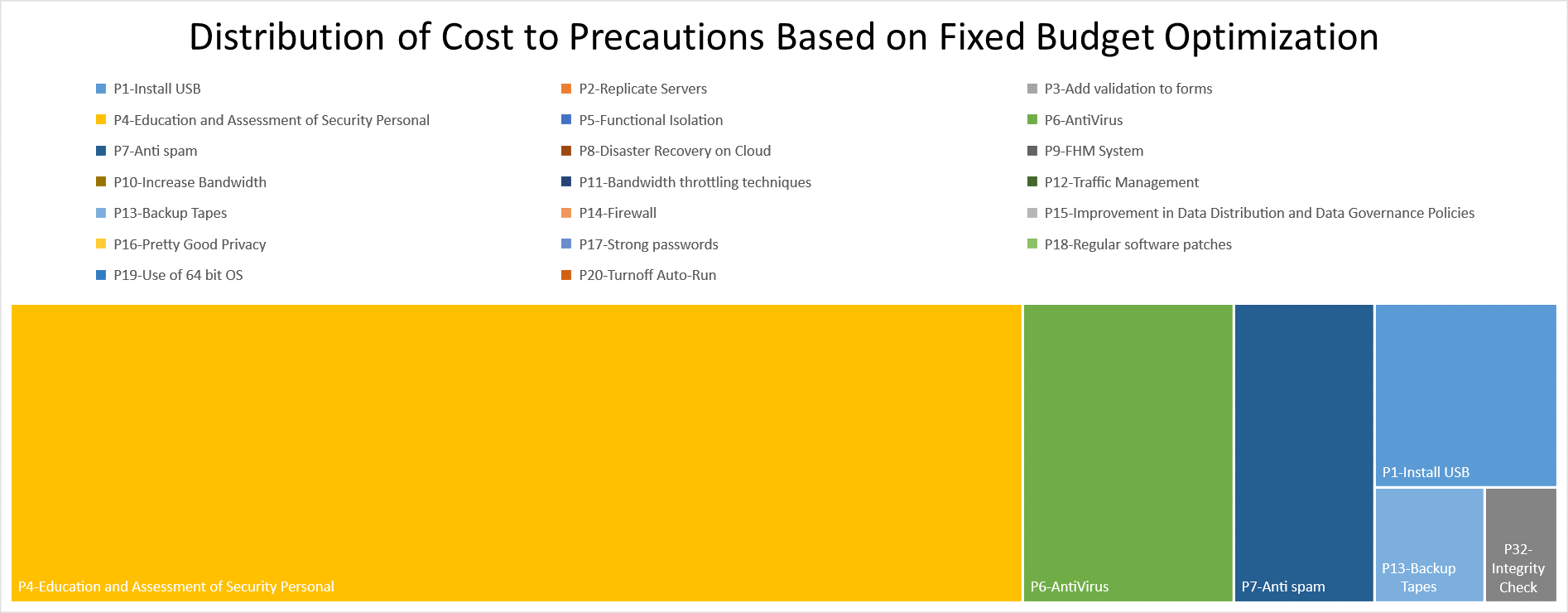


Visualizations for 60000 Budget:









|  |
| --- |
| Step 8: Assign a maximum risk level this expenditure plan.  Inputs: Acceptable risk level for the organization based on examination results of Step 6.  Outputs: Maximum budget monetary value. |

|  |
| --- |
| Info 3: At this step the user may run the model for various risk levels. For demonstration purposes OPISPA-V LP Optimization 2 is executed for %100 and %70 risk levels for the same threats using the same precautions and constraints. |

Minimum Acceptable Risk Level for Sample Case 4 = %100

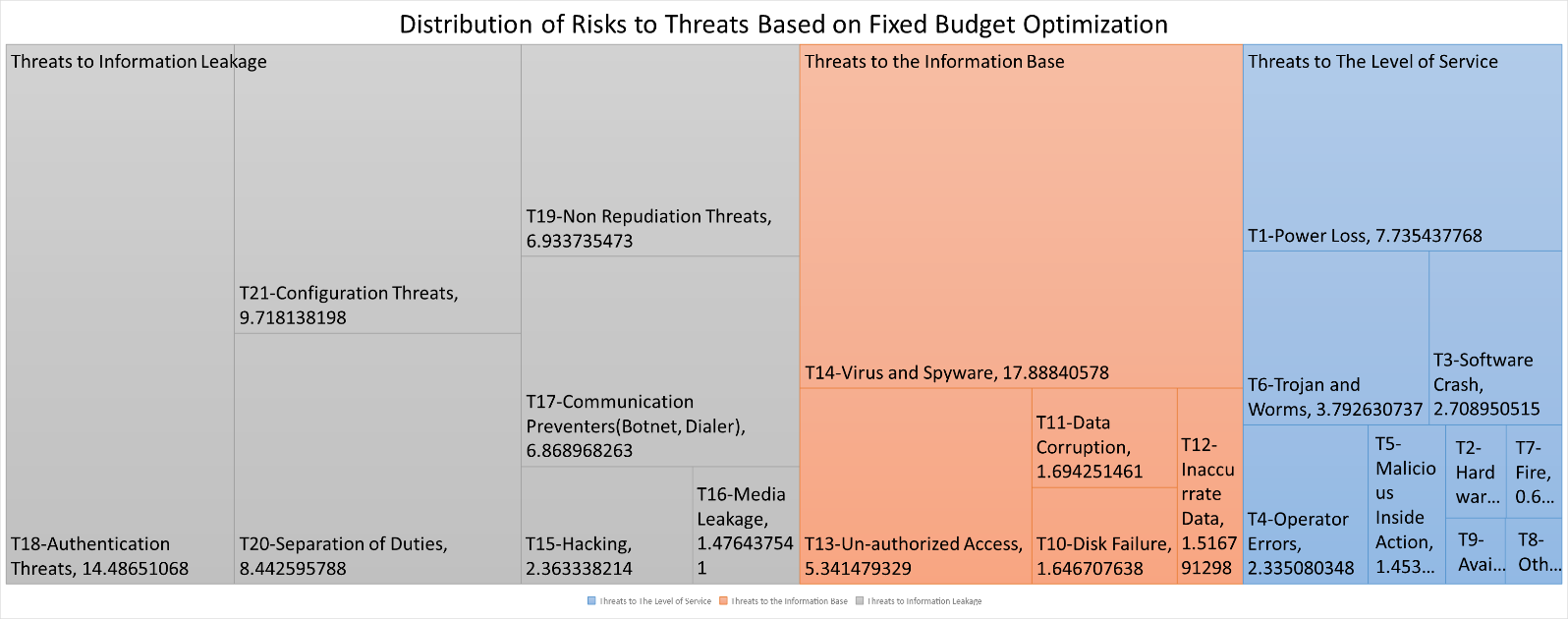
Minimum Acceptable Risk Level for Sample Case 5 = %70

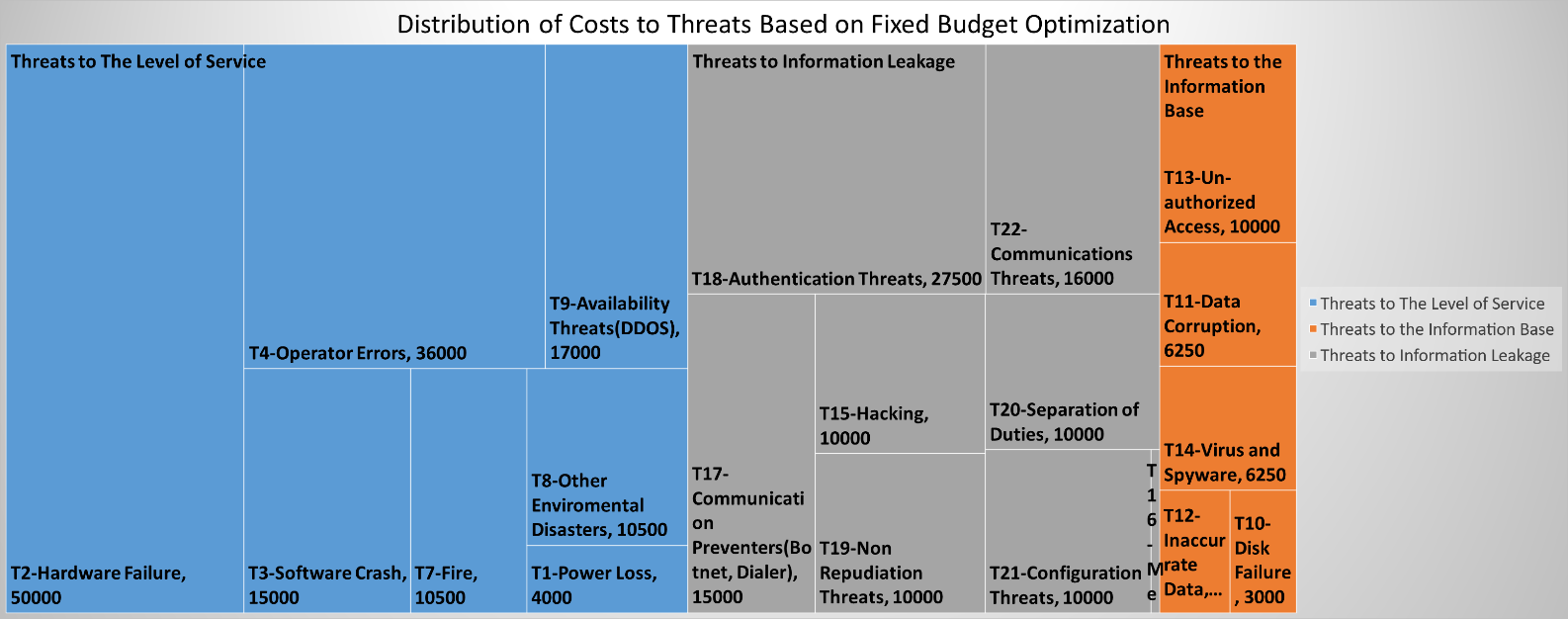
|  |
| --- |
| Step 9: Run optimization type 2 to determine best precaution choices for the fixed risk option.  Inputs: Threats, risks, precautions, risk level.  Outputs: Selected precautions with units and costs |

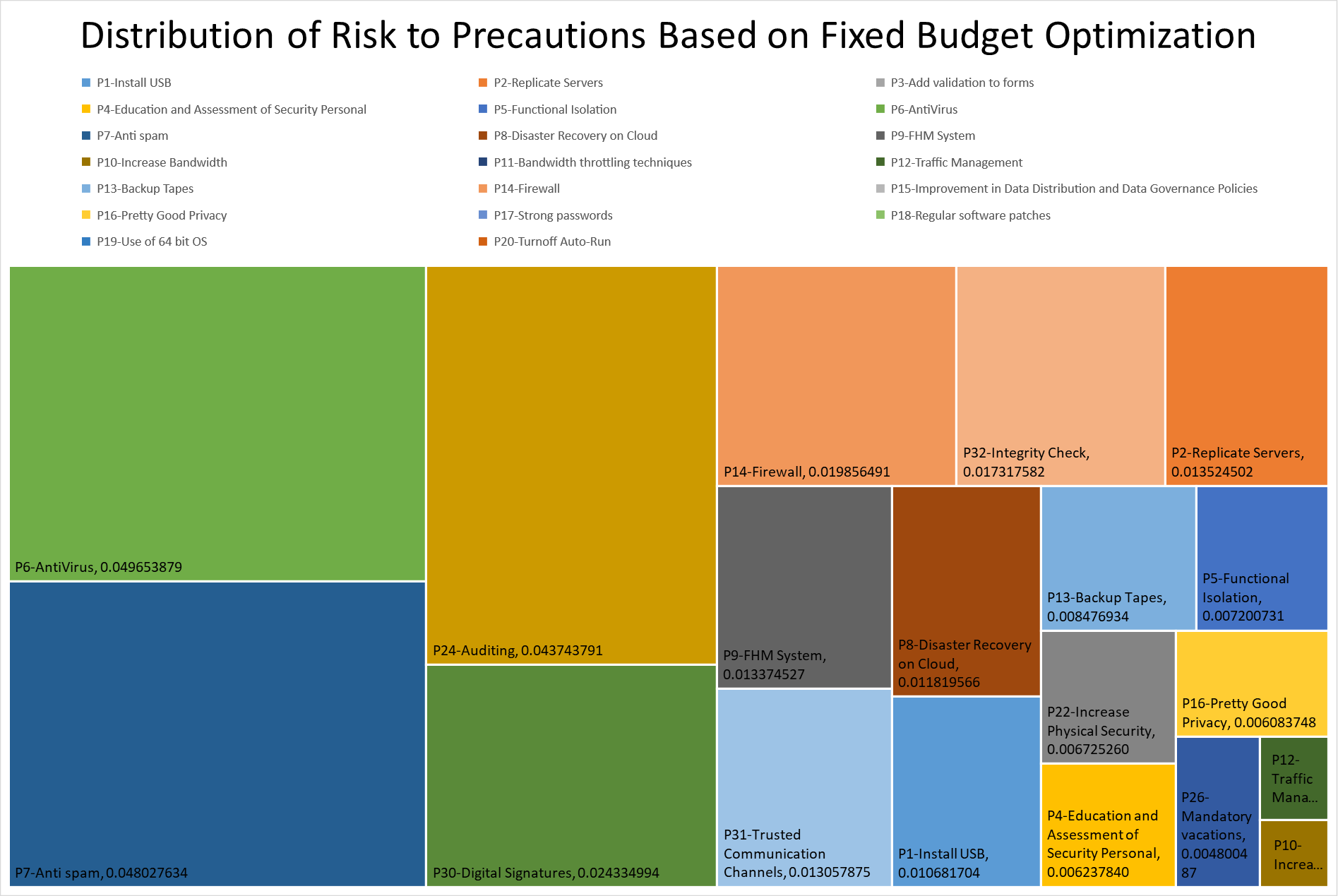
|  |  |  |
| --- | --- | --- |
|  | Minimum Acceptable Risk Level % 100 | Minimum Acceptable Risk Level % 70 |
| Budget Spent | 270700 | 89000 |
| Number of Threats Handled | 22 | 16 |
| Eliminated Risks(Tx) | T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T13, T14, T15, T16, T17, T18, T19, T20, T21, T22 | T1,T3,T4,T5,T6,T10,T11,T13,T14,T15,T16,T18,T19,T20,T21, T22 |
| Percentage of Eliminated Risk over Total Risk | %100 | %70 |
| Selected Pecautions by Optimization(Px(unit)) | P1(1), P2(5), P4(3), P5(1), P6(50), P7(50), P8(2), P9(2), P10(6), P11(3), P12(1), P13(6), P14(1), P15(4), P16(3), P17(1), P18(1), P19(1), P20(1), P21(1), P22(2), P23(1), P24(2), P25(1), P26(1), P27(2), P28(1), P28(2), P29(1), P30(1), P31(5), P32(1), P33(2) | P1(1), P4(3), P5(1), P6(50), P7(50), P13(2), P17(1), P18(1), P19(1), P20(1), P21(1), P22(1), P24(1), P25(1), P26(1), P27(2), P30(1), P32(1), P33(2) |

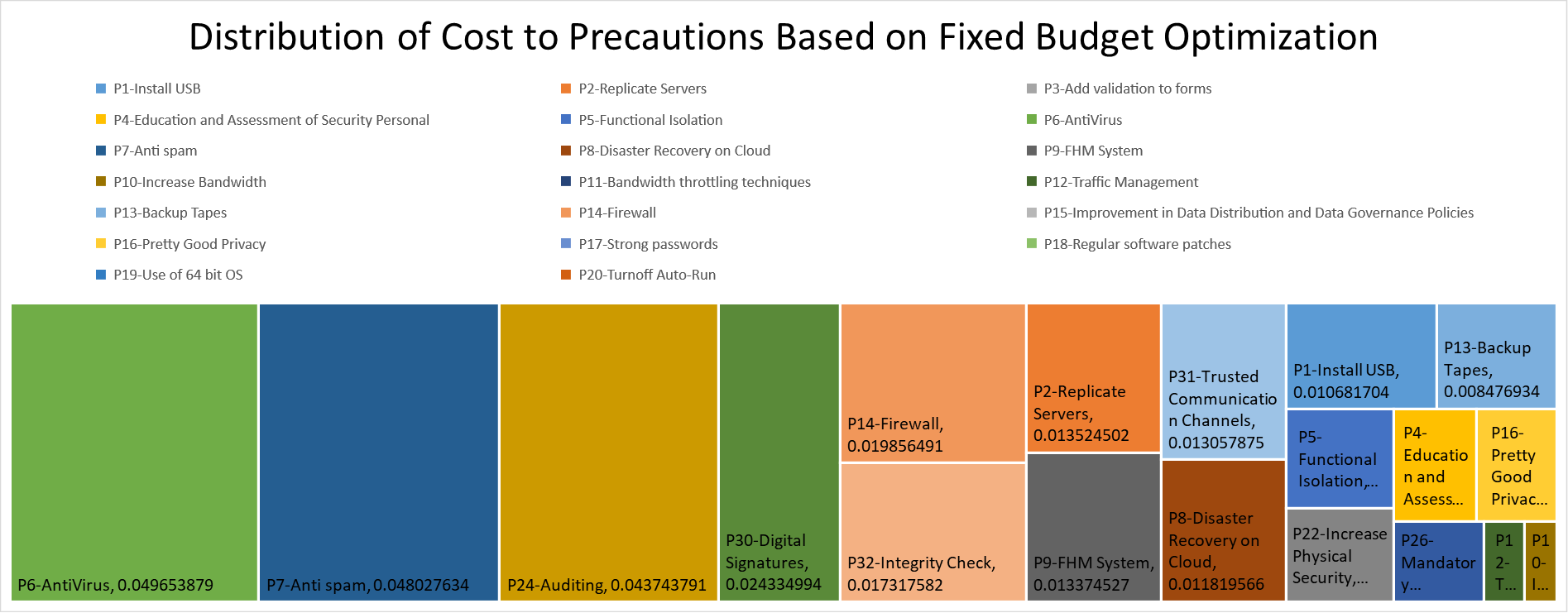
|  |
| --- |
| Step 10: Run visualization type 2 to examine the distribution in fixed risk option.  Inputs: Threats, risks, precautions, costs, units  Outputs: Visualizations for fixed risk plan |

Visualizations for Minimum % 100 Risk Coverage Level:

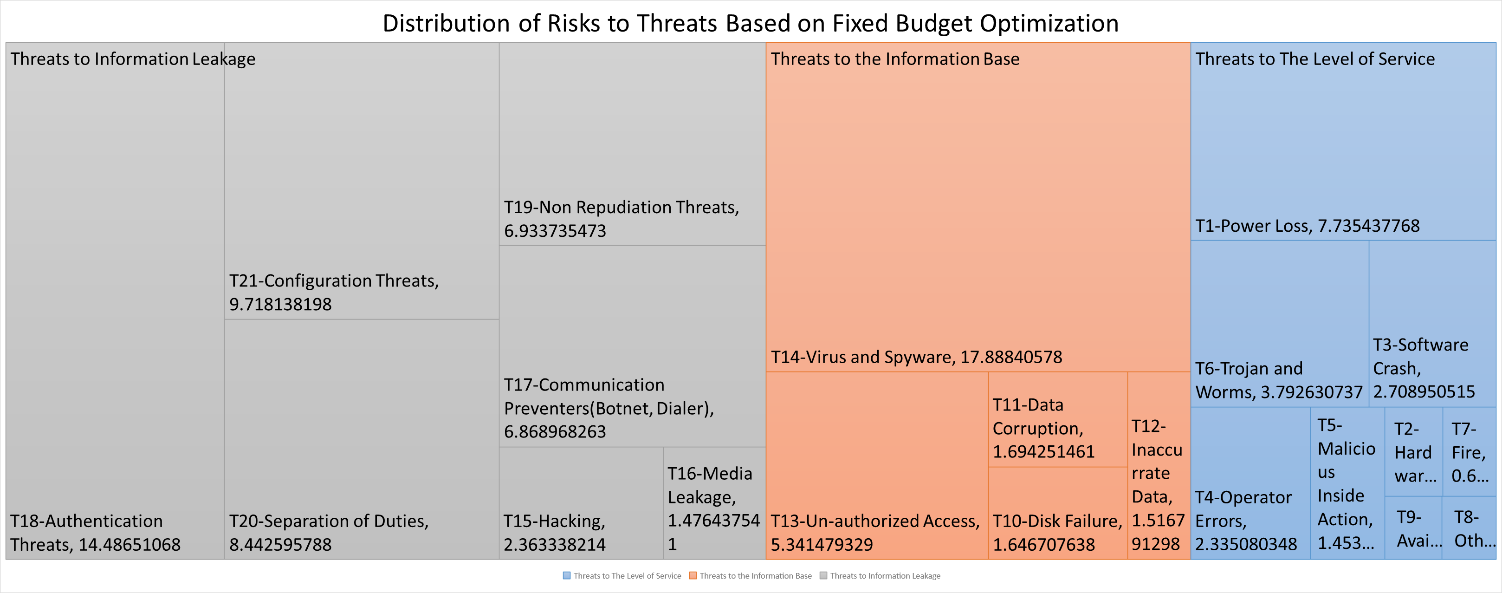


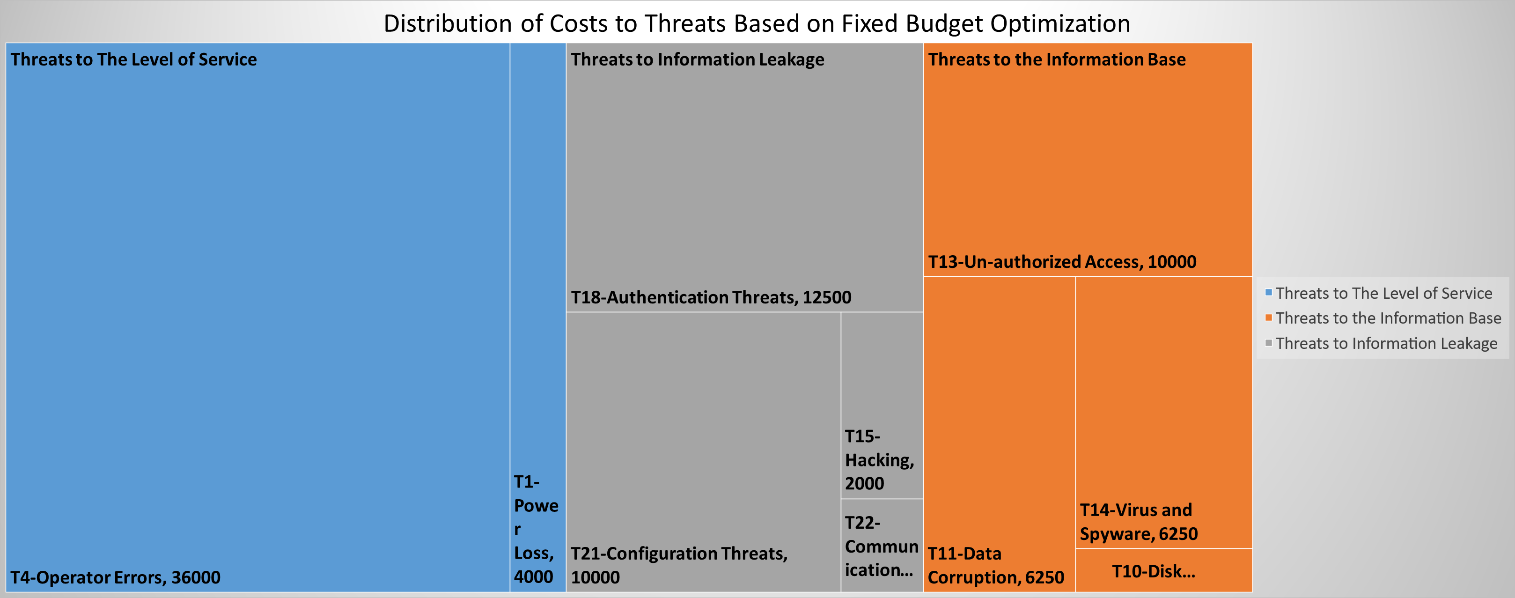


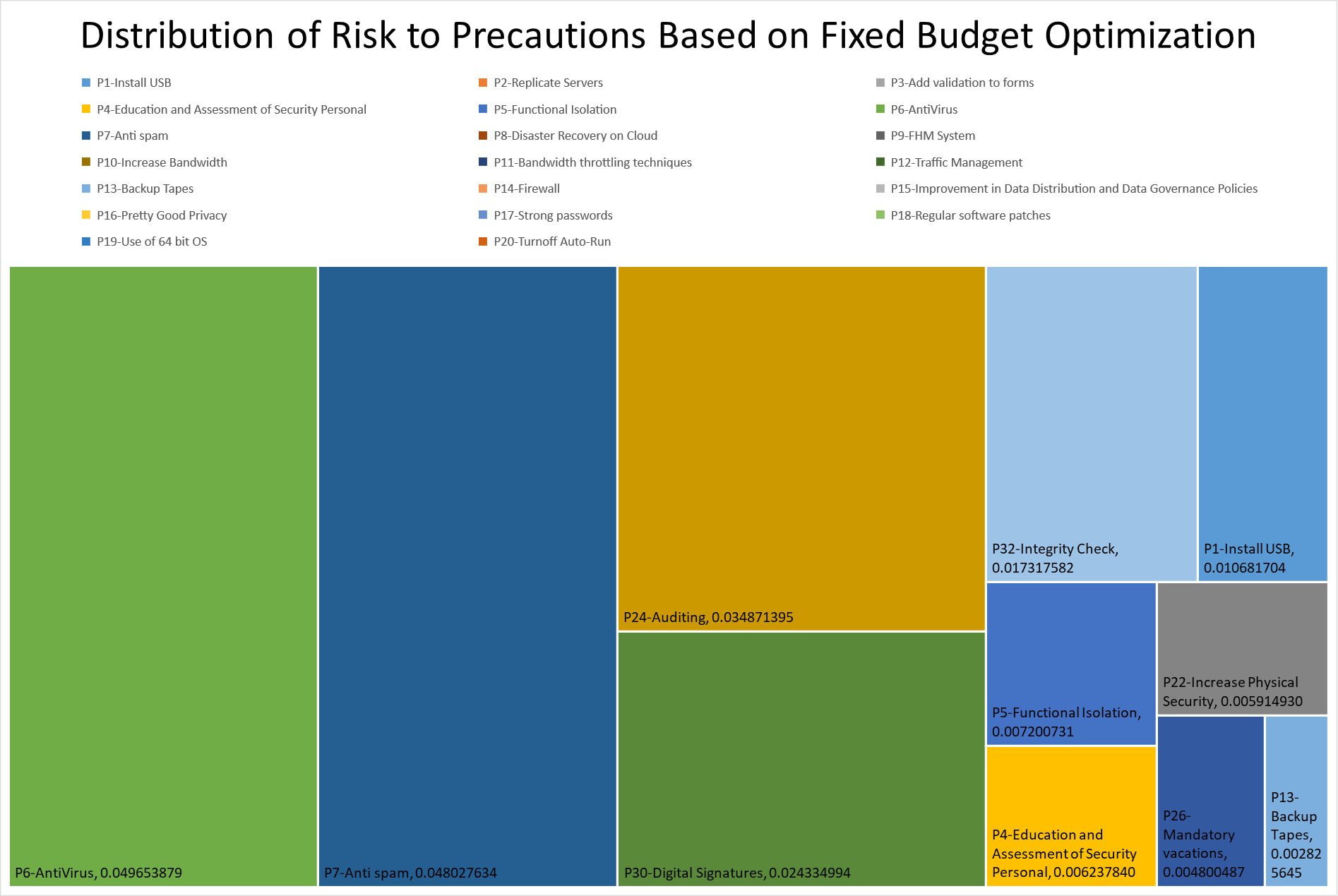


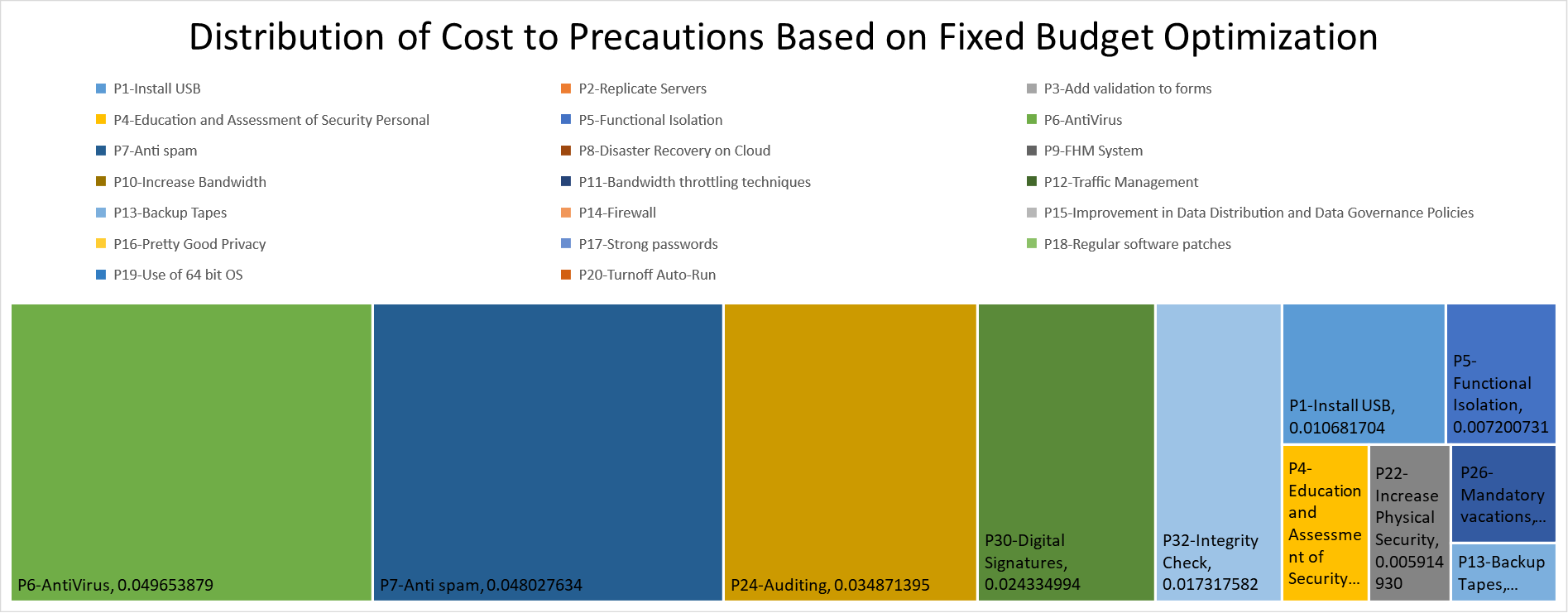


Visualizations for Minimum % 70 Risk Coverage Level:









|  |
| --- |
| Step 11: Change decision parameters. |

|  |
| --- |
| Question 3: Do you think visualization the distribution of risk and costs to the precautions and threats for various options would help to make better decisions more effectively during the precaution and budget selections?  Yes …………. No ………….. |

|  |
| --- |
| Info 4:The user may change any of the inputs at this step and return to appropriate previous step to re make the analyses. |