

Cybersecurity with Bayesian Networks

Corey Neskey

Likelihood Ratings			Impact Ratings	
Score	Description		Score	Description
1	Remote		1	Negligible
2	Unlikely		2	Acceptable
3	Possible		3	Unacceptable
4	Likely		4	High
5	Almost Certain		5	Unrecoverable

“Probability x Impact = Risk”

	A	B	C	D	E		G
1	Event Part I	Event part II	Probability	Impact	Prob. Val.	Imp. Val.	Risk
2	Malicious email attachment is opened	Keylogger malware sends all keystrokes to hacker.	Likely ▼	Average Impact ▼	3	3	9
3	Hacker guesses password	Password guessed.	Most Likely to Occur ▼	High Impact ▼	5	5	25
4	Hacker gets username/password via phishing attack	All files accessible with username and password are posted publically.	Good Chance ▼	High Impact ▼	4	5	20

1. Install anti-virus
2. Use strong passwords
3. Cybersecurity training



Likelihood

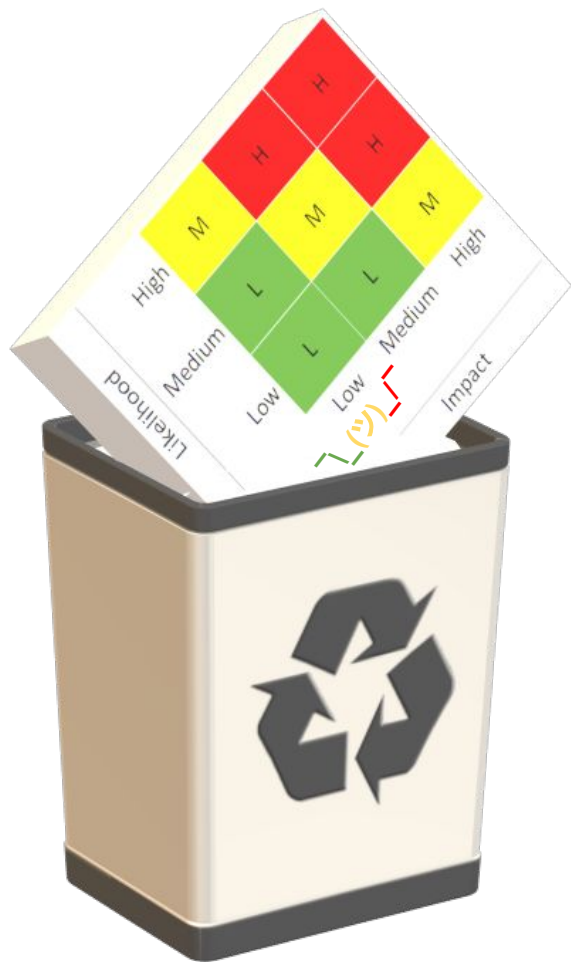
Medium

High

Low

High	M	H	H
Medium	L	M	H
Low	L	L	M
	Low	Medium	High

Impact

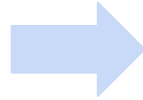


Inputs



Likelihood Ratings			Impact Ratings	
Score	Description		Score	Description
1	Remote		1	Negligible
2	Unlikely		2	Acceptable
3	Possible		3	Unacceptable
4	Likely		4	High
5	Almost Certain		5	Unrecoverable

Single Point Ordinal Scoring



Timeframe		Frequency Format	Percentage Format	Lower Bound	Most Likely	Upper Bound
Occurrences	(years)					
2	in 7	2/7	29%	\$ 1,700,000	\$ 4,300,000	\$ 6,000,000

Frequency format and confidence intervals





Loss Events

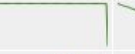
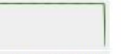
UID	Assets at risk	Containers/Points of attack	Threat communities	Threat Types	Effects	Control(s)	Lower Bound	Most Likely	Upper Bound	Lower Bound	Most Likely	Upper Bound
Risk-1	Non Public Information (NPI)	Subnet Neighbors on Oak-Net	privileged insiders (DerpCorp & Vendors)	deliberately	confidentiality	Crit. sec. patches monthly, OS MFA, App MFA, Net ACL/FW Default Deny IN,	1 in 75	1 in 20	1 in 2	\$750,000	\$3,000,000	\$10,000,000
Risk-2	Non Public Information (NPI)	ServerGaugeMgmt Server on Oak-Net	privileged insiders (DerpCorp & Vendors)	deliberately	confidentiality	Crit. sec. patches monthly, OS MFA, App MFA, Net ACL/FW Default Deny IN,	1 in 75	1 in 20	1 in 2	\$750,000	\$3,000,000	\$10,000,000
Risk-3	Non Public Information (NPI)	ServerGaugeReport Server on Oak-Net	privileged insiders (DerpCorp & Vendors)	deliberately	confidentiality	Crit. sec. patches monthly, OS MFA, App MFA, Net ACL/FW Default Deny IN,	1 in 75	1 in 20	1 in 2	\$750,000	\$3,000,000	\$10,000,000
Risk-4	Non Public Information (NPI)	ServerGaugeIndex Server on Oak-Net	privileged insiders (DerpCorp & Vendors)	deliberately	confidentiality	Crit. sec. patches monthly, OS MFA, App MFA, Net ACL/FW Default Deny IN,	1 in 75	1 in 20	1 in 2	\$750,000	\$3,000,000	\$10,000,000

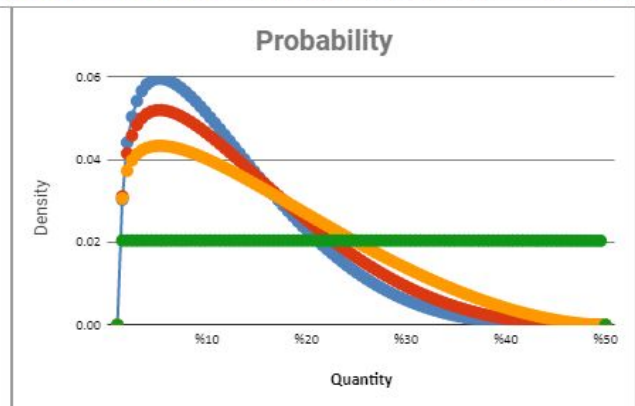
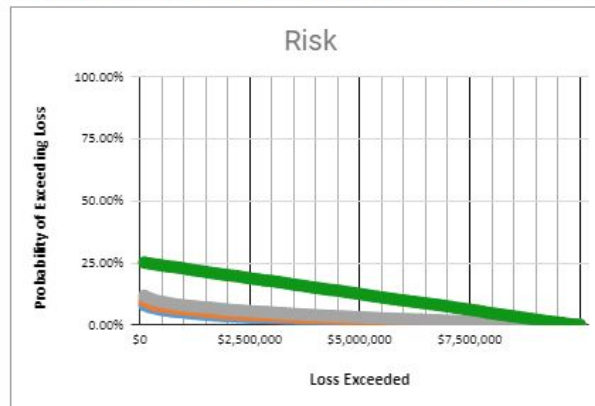
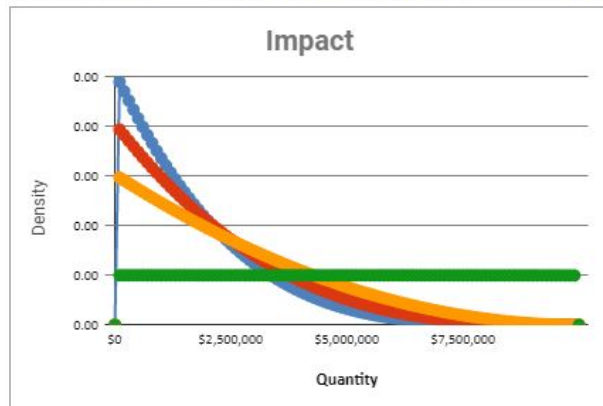


Generated Scenarios

Security Controls

Estimates

	Impact	Risk	Probability	Simulations:								
Max Possible	\$10,000,000		50.00									
Most Likely	\$10,000		5.00									
Minimum Possible	\$8,000		1.00									
Peakedness	4	4	4	3	3	3	2	2	2	0.001	0.001	0.001
a	1.000800641		1.326530612	1.00060048		1.244897959	1.00040032		1.163265306	1.0000002		1.000081633
b	4.999199359		4.673469388	3.99939952		3.755102041	2.99959968		2.836734694	1.0009998		1.000918367
Random	\$1,944,181		42.37	\$9,920,759		49.98	\$9,546,416		5.07	\$1,875,876		41.36
Distribution shape												
Simulation Min	\$8,000	\$0	1.00	\$8,000	\$0	1.0000000	\$8,000	\$0	1.0000000	\$8,533	\$0.00	1.0021499
Simulation Mean	\$1,678,120.59	\$223,032.85	11.94	\$2,048,433	\$281,312	13.0778100	\$2,442,932	\$381,485	15.0301842	\$4,953,116	\$1,250,828.07	25.4256461
Simulation Median	\$319,593	\$0	4.24	\$659,281	\$0	6.1726461	\$1,213,679	\$0	9.1312680	\$4,956,999	\$0.00	25.2023013
Simulation 75th perc	\$2,394,818	\$0	18.89	\$3,267,292	\$0	21.6608868	\$4,000,869	\$0	25.3875360	\$7,422,438	\$140,017.34	37.8240100
Simulation Max	\$9,995,209	\$9,972,760	50.00	\$9,998,252	\$9,964,098	49.9984927	\$9,994,726	\$9,987,486	49.9851302	\$9,999,759	\$9,998,486.13	49.9998690
Simulation Range	\$9,987,209	\$9,972,760	49.00	\$9,990,252	\$9,964,098	48.9984927	\$9,986,726	\$9,987,486	48.9851302	\$9,991,226	\$9,998,486.13	48.9977191

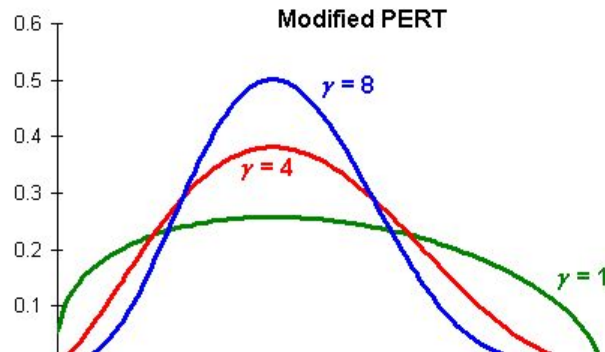


Format: ModPERT(min, mode, max, g)

The Modified PERT distribution was first proposed in Vose (2000). It is a modification of the [PERT distribution](#) with minimum a, most likely b and maximum c to produce shapes with varying degrees of uncertainty for the a,b,c values by changing the assumption about the mean:

$$\text{The mean } (\mu) = \frac{a + \gamma * b + c}{\gamma + 2}$$

In the standard PERT, $\gamma = 4$, which is the PERT network assumption that the best estimate of the duration of a task = $(a + 4b + c) / 6$. However, if we increase the value of γ , the distribution becomes progressively more peaked and concentrated around b (and therefore less uncertain). Conversely, if we decrease γ the distribution becomes flatter and more uncertain. The figure below illustrates the effect of three different values of γ for a modified PERT(5,7,10) distribution.



<https://www.vosesoftware.com/riskwiki/ModifiedPERTdistribution.php>

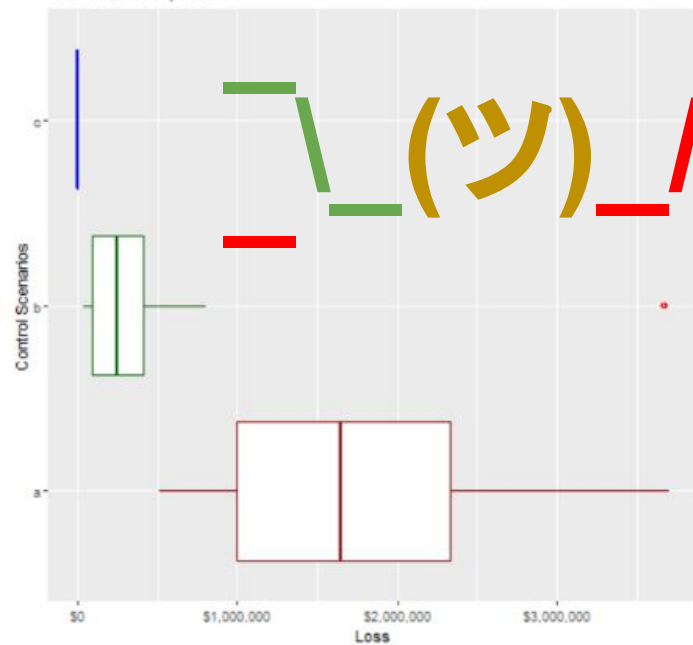
Ordinal Scoring

Likelihood	High	M	H	H
	Medium	L	M	H
	Low	L	L	M
		Low	Medium	High

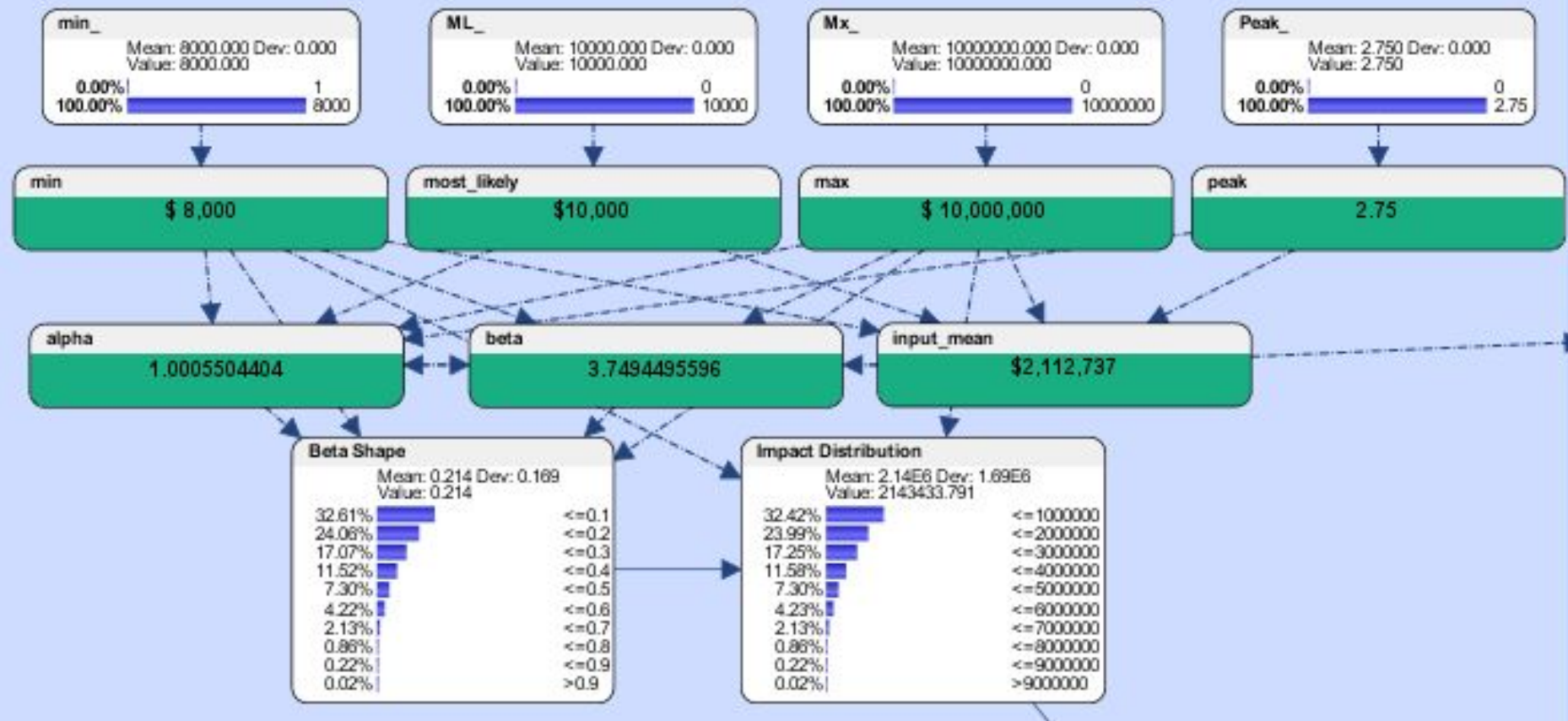
Impact



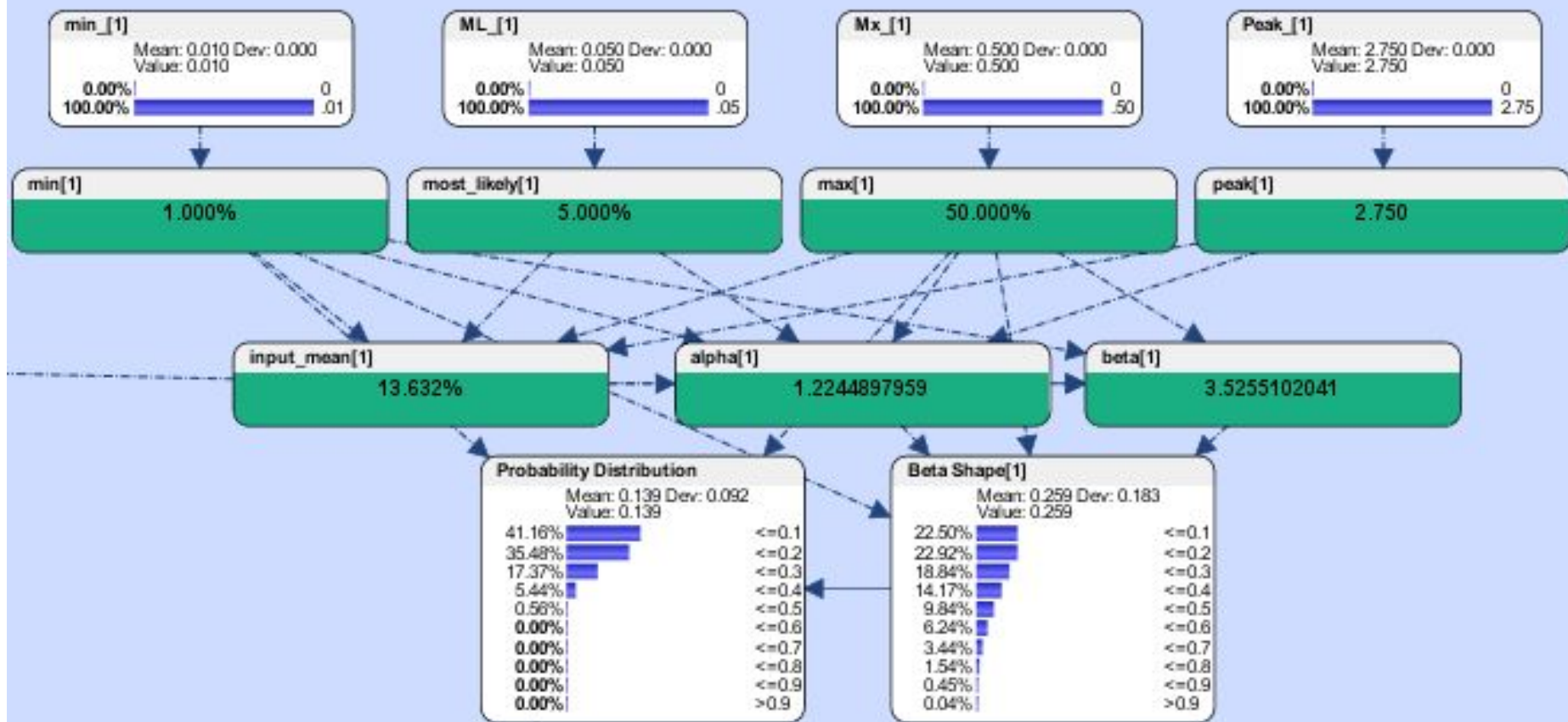
Simulated Loss Output
Over a 12 month period



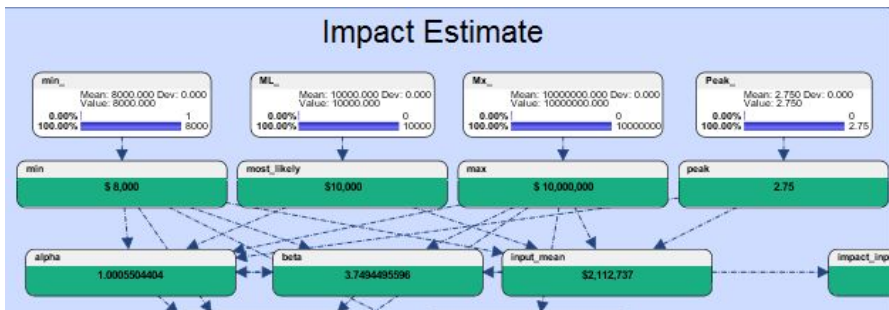
Impact Estimate



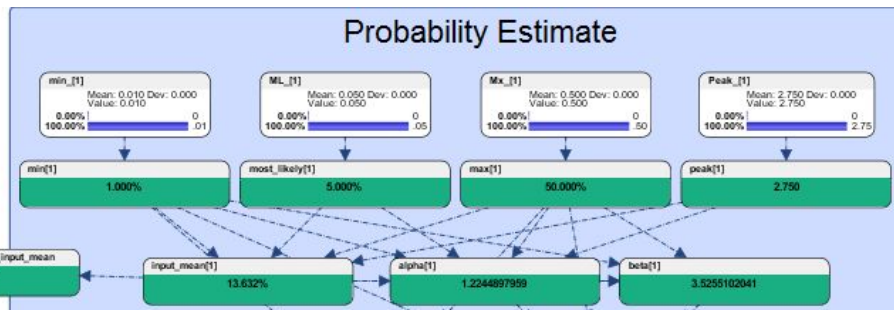
Probability Estimate



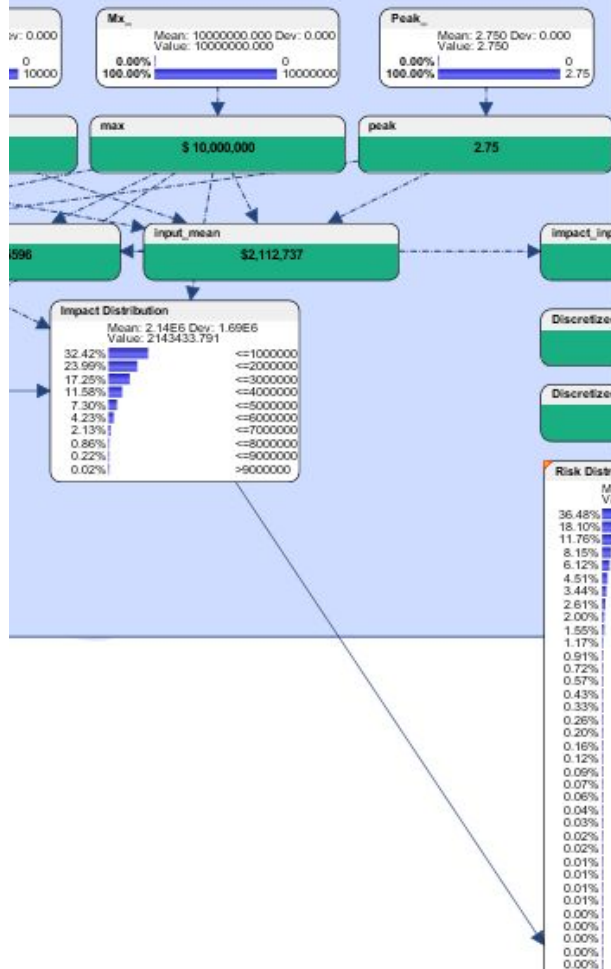
Impact Estimate



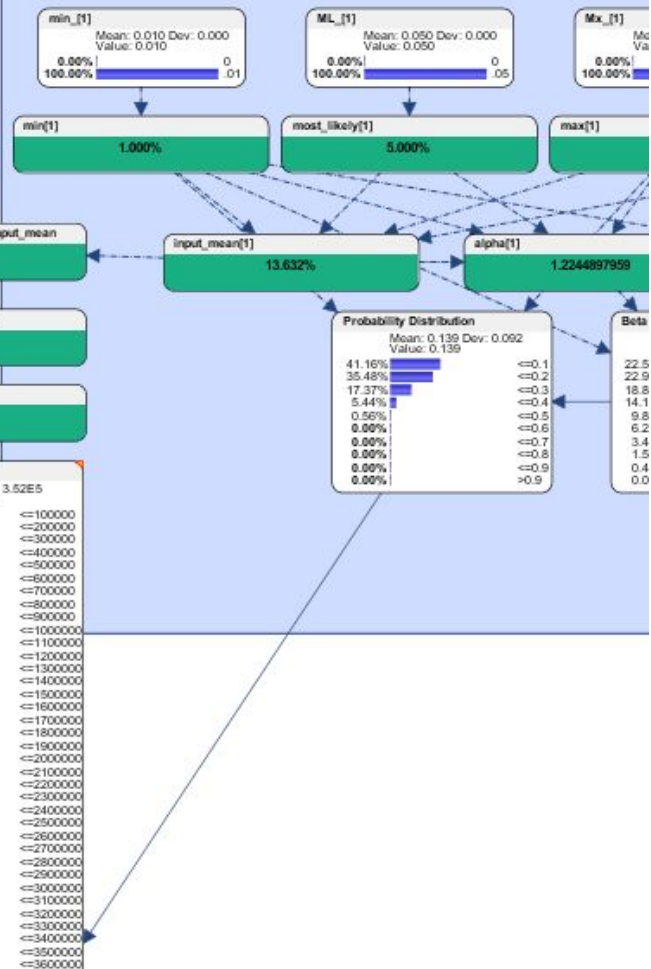
Probability Estimate

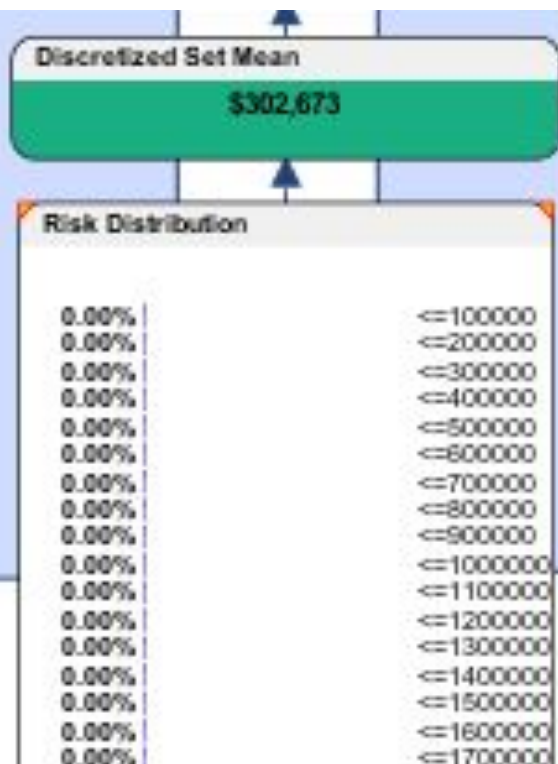


Estimate



Probability Est





Node Editor

States

Probability Distribution

Properties

Classes

Values

Stat

Probabilistic

Deterministic

Tree

Equation

Updating

Equation Type: ☒ Deterministic ☐ Probabilistic

?Risk Distribution? =

?Probability Distribution?*?Impact Distribution?

impact_input_mean*prob_input_mean

\$287,999

Discretized Vs Input mean

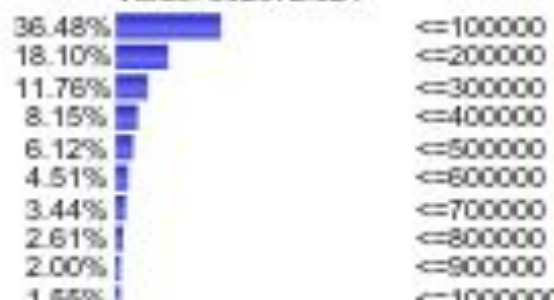
\$14,673

Discretized Set Mean

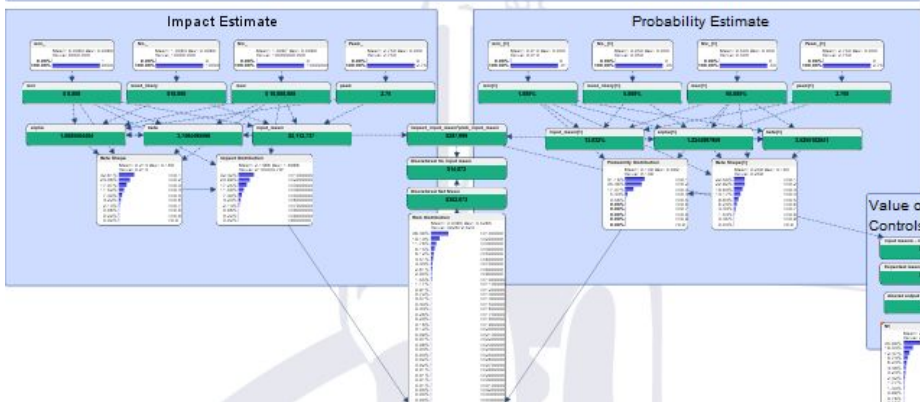
\$302,673

Risk Distribution

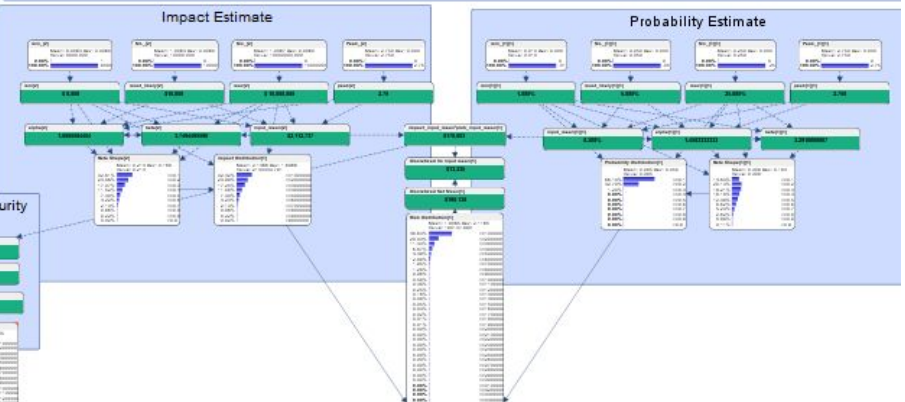
Mean: 3.03E5 Dev: 3.52E5
Value: 302672.524



Current Risk	
--------------	--



Risk after you install anti-virus software, firewalls, multi-factor-authentication



Value of Security Controls

input means - input means

\$232,401

Expected mean vs dist mean

\$51,700

discret output mean

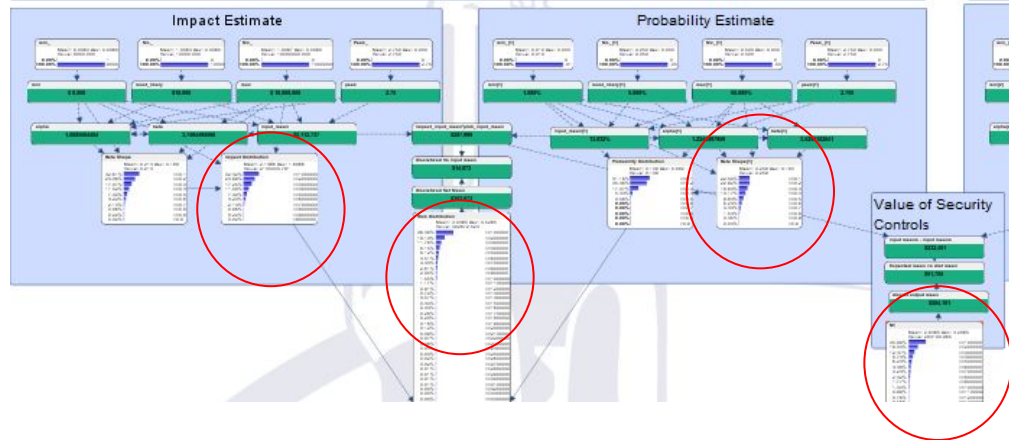
\$284,101

H1

Mean: 284100.965 Dev: 320448.868
Value: 284100.965

35.88%		<=100000
19.34%		<=200000
12.47%		<=300000
8.74%		<=400000
6.24%		<=500000
4.48%		<=600000
3.24%		<=700000
2.42%		<=800000
1.77%		<=900000
1.33%		<=1000000
0.98%		<=1100000
0.76%		<=1200000

Current Risk



Risk after you install anti-virus software, firewalls, multi-factor-authentication

