INTRODUCTION TO THE CYBERRISKMODELS.COM EDUCATIONAL BUNDLE

Charlene Deaver-Vazquez, President
FISMACS, LLC
Charlene@CyberRiskModels.com

Cyber Risk Models.com

TABLE OF CONTENTS

INTRODUCTION

Our Story

The genesis of our educational bundle stems from my tenure at the Nuclear Regulatory Commission, where I was tasked with risk quantification responsibilities. However, during this endeavor, I encountered a noticeable void in the availability of affordable, accessible tools designed for this purpose. The alternative was mastering a new coding language, a path that was not desirable in my circumstances. This scenario presented a unique challenge that sparked the development of a proprietary set of analytical tools, custom-built to meet my professional requirements. These are now at the heart of our educational bundle, meticulously designed and continuously refined to deliver superior value and efficiency.

To learn more, visit our website CyberRiskModels.com and our YouTube channel @CyberRiskModels.

What's Included

The Education Bundle from CyberRiskModels.com includes a variety of tools and is designed to help the cyber professional quickly and easily quantify cyber risk.

The Models

- Probability Calculator
- Joint Probability
- Bayesian Inference
- Probability Tree
- Probability Distributions
- FAIR™
- Vulnerability Analysis
- Compliance Risk
- Industry Attacks
- Attack Scenario

About The Models

Probability Calculator

The probability calculator is a quick and easy resource that allows you to calculate many of the conditional probability formulas. To use the formulas, you only need to know the values of two events (A and B).

It is very useful to be able to calculate the probability of events occurring. By calculating the likelihood of two events occurring together, we can make more informed forecasts and decisions.

For example, in finance, calculating the joint probability of two investments can help us determine the overall risk of a portfolio. In engineering, understanding the probability of two components failing at the same time can help us design more reliable systems. In health care, calculating the probability of two risk factors occurring together can help us identify patients who are at a higher risk for certain diseases, and in cyber security, having the ability to calculate the joint probability of a threat and the likelihood allows us to quantify the risk of a negative event.

Joint Probability

The joint probability allows you to easily calculate the probability of two events occurring. For cyber security, we will think of these as threats and likelihood. This tool provides an easy-to-use educational layout that helps you understand combinations of probabilities. Here you will spin, and the same calculations are explored as are found in the probability calculator. The layout of the joint probability tool is what I call the probability box. You will use this tool many times in calculating risk. By employing the joint probability formula: Threat × Likelihood = Risk, which represents the essence of joint probability, you can utilize the joint probability when the values for both events A and B are known. These input values of A and B form the foundation of this model.

Bayesian Inference

Joint probability and Bayesian inference are two related concepts in probability theory, but they differ in their approach and application.

A joint probability is a measure of the probability of two or more events occurring together. It is calculated by multiplying the probability of each individual event. For example, suppose we want to calculate the joint probability of rolling a 1 on a fair die and flipping a head on a fair coin. In that case, we will multiply the probability of rolling a 1 (1/6) by the probability of flipping a head (1/2), resulting in a joint probability of 1/12.

On the other hand, Bayesian inference is a method for updating our beliefs about the probability of an event occurring based on new evidence or information. It involves using Bayes' Theorem to calculate the posterior probability distribution, which represents our updated beliefs about the probability of the event. Bayesian inference takes into account prior knowledge or beliefs about the probability of the event, as well as new evidence or data.

The main difference between joint probability and Bayesian inference is that joint probability is a static measure of the probability of two or more events occurring together, whereas Bayesian inference is a dynamic method for updating our beliefs about the probability of an event based on new evidence or information.

Another difference is that joint probability is often used to calculate the probability of events that are independent of each other. In contrast, Bayesian inference calculates the probability of events that are not necessarily independent. Bayesian inference takes into account the relationship between events and how they affect each other, whereas joint probability assumes that events are independent of each other.

Joint probability and Bayesian inference are both important concepts in probability theory, but they differ in their approach and application. Joint probability is a static measure of the probability of two or more events occurring together, whereas Bayesian inference is a dynamic method for updating our beliefs about the probability of an event based on new evidence or information. Bayesian inference takes into account prior knowledge or beliefs about the probability of the event, as well as new evidence or data, and is used to calculate the probability of events that are not necessarily independent of each other.

Probability Tree

Probability trees, also known as decision trees, are a powerful tool for visualizing and calculating the probabilities of different outcomes in a complex decision-making process. They are commonly used in fields such as finance, engineering, and data science to model and analyze uncertain situations.

A probability tree consists of a series of branches that represent the different possible outcomes of a decision or event. Each branch is assigned a probability based on the likelihood of that

outcome occurring. The branches then split into further branches, representing the different possible outcomes of subsequent decisions or events.

By following the branches of the tree, we can calculate the probabilities of different outcomes and make informed decisions based on this information. Probability trees can also be used to calculate the expected value of different decisions, which is the sum of the probability of each outcome multiplied by its associated payoff.

One of the key benefits of probability trees is that they allow us to model complex decision-making processes in a clear and intuitive way. By breaking down a decision into its component parts and assigning probabilities to each outcome, we can gain a better understanding of the risks and rewards associated with different options.

Probability trees are a powerful tool for modeling and analyzing complex decision-making processes. They allow us to visualize the different possible outcomes of a decision, assign probabilities to each outcome, and calculate the expected value of different options. By using probability trees, we can make more informed decisions and better manage risk in uncertain situations.

Probability Distributions

Probability distributions are mathematical functions that describe the likelihood of different outcomes in a random event. They are used extensively in various fields, including finance, engineering, and science, to model and analyze data. In the field of cybersecurity, probability distributions are used to quantify the likelihood of cyber threats and their potential impact on an organization. We will discuss three probability distributions – Poisson, Triangular, and Bernoulli – and their use in quantifying cyber risk.

Poisson Distribution

The Poisson distribution is a discrete probability distribution that models the number of events that occur in a fixed interval of time or space. It is commonly used to model rare events that occur randomly, such as cyber attacks. The Poisson distribution is characterized by a single parameter, λ, which represents the average number of events that occur in the interval.

In the context of cybersecurity, the Poisson distribution can be used to model the frequency of cyber attacks. For example, if an organization experiences an average of ten cyber attacks per month, the Poisson distribution can be used to calculate the probability of experiencing a certain number of attacks in a given time period. This information can be used to estimate the likelihood of a successful cyber attack and to develop appropriate risk management strategies.

Triangular Distribution

The triangular distribution is a continuous probability distribution commonly used to model uncertain variables with a known minimum, maximum, and mode. It is characterized by three parameters – a, b, and c – which represent the minimum, maximum, and mode of the distribution, respectively.

In cybersecurity, the triangular distribution can be used to model the potential impact of a cyber attack. For example, the impact of a cyber attack on an organization can be uncertain. It may depend on several factors, such as the type of attack, the target system, and the security measures in place. The triangular distribution can be used to model this uncertainty and estimate the potential impact of a cyber attack on the organization.

Bernoulli Distribution

The Bernoulli distribution is a discrete probability distribution that models a random variable that takes on one of two possible values – 0 or 1. It is commonly used to model binary events, such as success or failure, or the presence or absence of a cyber attack in the context of cybersecurity.

In cybersecurity, the Bernoulli distribution can be used to model the likelihood of a successful cyber attack. For example, if an organization has a vulnerability that a cyber attacker can exploit, the Bernoulli distribution can be used to model the probability of a successful attack. This information can be used to estimate the likelihood of a successful attack and to develop appropriate risk management strategies.

Probability distributions are an essential tool for quantifying cyber risk. They provide a mathematical framework for modeling the likelihood of cyber threats and their potential impact on an organization. The Poisson distribution can be used to model the frequency of cyber attacks, the triangular distribution can be used to model the potential impact of a cyber attack, and the Bernoulli distribution can be used to model the likelihood of a successful cyber attack. By using these probability distributions, organizations can better understand their cyber risk and develop appropriate risk management strategies to mitigate the impact of cyber threats.

FAIR™

The FAIR (Factor Analysis of Information Risk) standard is a quantitative framework for assessing and managing information risk. It provides a methodology for estimating the probability and impact of potential cyber attacks, allowing organizations to make informed decisions about how to allocate resources and manage risk effectively.

The FAIR standard consists of six steps: scoping, assessing the threat landscape, identifying risk scenarios, estimating the frequency of loss events, estimating the magnitude of loss events, and calculating the risk.

The first step, scoping, involves defining the scope of the risk assessment, including the assets, threats, and scenarios that will be evaluated.

The second step, assessing the threat landscape, involves identifying the potential threats that could impact the organization, such as phishing attacks, malware infections, or denial of service attacks.

The third step, identifying risk scenarios, involves developing specific scenarios that describe how each threat could impact the organization. These scenarios should be realistic and based on historical data or industry trends.

The fourth step, estimating the frequency of loss events, involves assessing the likelihood that each risk scenario will occur. This involves examining the controls in place to prevent or mitigate the risk, as well as the external threat environment.

The fifth step, estimating the magnitude of loss events, involves assessing the potential impact of each risk scenario. This could include financial losses, reputational damage, or legal liability.

Finally, the sixth step, calculating the risk, involves combining the probability and impact estimates to arrive at a quantitative estimate of the risk. This can be expressed in financial terms, such as the expected loss over a given time period.

One of the key benefits of quantifying cyber risk in financial terms is that it allows organizations to prioritize their risk management efforts based on the potential impact of each risk scenario. By expressing the risk in financial terms, organizations can compare the potential impact of different risk scenarios and allocate resources accordingly.

For example, if a risk assessment reveals that a particular risk scenario could result in a $1 million loss, while another scenario could result in a $100,000 loss, the organization can prioritize efforts to mitigate the higher impact scenario. This could involve investing in additional security controls, implementing more rigorous training programs for employees, or purchasing cyber insurance to mitigate the financial impact of the risk.

Another benefit of quantifying cyber risk in financial terms is that it allows organizations to communicate the potential impact of cyber risk to senior management and other stakeholders. By expressing the risk in financial terms, organizations can more effectively communicate the potential impact of cyber risk and the importance of investing in risk management efforts.

The FAIR standard provides a quantitative framework for assessing and managing cyber risk. By quantifying the probability and impact of potential cyber attacks, organizations can make informed decisions about how to allocate resources and manage risk effectively. By expressing the risk in financial terms, organizations can prioritize their risk management efforts and communicate the potential impact of cyber risk to senior management and other stakeholders.

Vulnerability Analysis

Vulnerability analysis is a process of identifying and assessing vulnerabilities in a system or network that could be exploited by attackers. In the context of cyber risk, vulnerability analysis is an essential component of risk management, as it helps organizations identify potential weaknesses in their security controls and prioritize their allocation of resources for mitigating risk.

Vulnerability analysis involves a variety of techniques, including vulnerability scanning, penetration testing, and risk assessments. Vulnerability scanning involves using automated tools to scan a system or network for known vulnerabilities, such as outdated software or misconfigured settings. Penetration testing involves simulating an attack on a system or network to identify vulnerabilities that may not be detected by automated tools. Risk assessments involve evaluating the potential impact of a vulnerability and the likelihood of it being exploited by an attacker.

By conducting vulnerability analysis, organizations can identify potential weaknesses in their security controls and prioritize their allocation of resources for mitigating risk. For example, if a vulnerability analysis reveals that a particular system is running outdated software that is vulnerable to exploitation, the organization can prioritize efforts to update the software or implement additional security controls to mitigate the risk.

Vulnerability analysis is also important for ensuring that organizations are compliant with industry regulations and standards. Many regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), require organizations to conduct regular vulnerability assessments to identify and address potential security weaknesses.

In addition, vulnerability analysis can help organizations make informed decisions about investing in new security technologies or services. By identifying potential vulnerabilities and the impact of those vulnerabilities, organizations can determine the most effective way to allocate their resources for mitigating risk.

Vulnerability analysis is an essential component of cyber risk management. By identifying potential vulnerabilities and assessing their impact and likelihood of exploitation, organizations

can prioritize their allocation of resources for mitigating risk. This can help organizations ensure compliance with industry regulations and standards, as well as make informed decisions about investing in new security technologies or services.

Compliance Risk

Compliance risk refers to the potential for an organization to violate laws, regulations, or industry standards that govern their operations. Compliance risk can arise from a variety of sources, including changes in regulations, inadequate policies or procedures, or lack of employee training. Quantifying compliance risk is important for organizations as it helps them identify areas of non-compliance and prioritize their efforts to mitigate the risk.

Quantifying compliance risk involves assessing the potential impact of non-compliance and the likelihood of it occurring. This can be done by reviewing regulations and standards that apply to the organization, identifying areas of non-compliance, and evaluating the potential impact of non-compliance on the organization's operations and reputation.

By quantifying compliance risk, organizations can prioritize their risk management efforts and focus on what is most important. For example, if a compliance risk assessment reveals that the organization is at substantial risk for violating a particular regulation, they can allocate resources to ensure compliance with that regulation. This could involve implementing new policies or procedures, providing employee training, or investing in innovative technologies to ensure compliance.

Quantifying compliance risk also helps organizations avoid potential financial and reputational losses that can result from non-compliance. Non-compliance can result in fines, legal action, and damage to the organization's reputation. By identifying areas of non-compliance and prioritizing efforts to mitigate the risk, organizations can avoid these potential losses and maintain their reputation as a compliant and ethical business.

Another benefit of quantifying compliance risk is that it helps organizations demonstrate their commitment to compliance to stakeholders, including regulators, customers, and investors. By conducting regular compliance risk assessments and taking steps to mitigate identified risks, organizations can demonstrate their commitment to compliance and build trust with stakeholders.

Quantifying compliance risk is a vital component of risk management for organizations. By identifying areas of non-compliance and prioritizing efforts to mitigate the risk, organizations can avoid potential financial and reputational losses, demonstrate their commitment to compliance, and focus on what is most important.

Industry Attacks

Modeling industry attacks is an important component of cyber risk management as it helps organizations identify potential threats and vulnerabilities and design effective mitigations to reduce overall cyber risk. Industry attack models are designed to simulate real-world cyber attacks and provide insights into the tactics, techniques, and procedures used by attackers.

By modeling industry attacks, organizations can identify potential vulnerabilities in their systems and networks and develop effective mitigations to reduce the risk of a successful attack. For example, if an industry attack model reveals that a particular type of malware is commonly used in cyber attacks, the organization can prioritize efforts to implement controls to prevent or detect the malware.

Modeling industry attacks also help organizations focus their efforts on what is most important. By understanding the tactics, techniques, and procedures used by attackers in their industry, organizations can prioritize their risk management efforts and allocate resources effectively. This can help organizations reduce overall cyber risk and ensure that their security controls are effective in mitigating potential threats.

In addition, modeling industry attacks can help organizations prepare for potential cyber attacks. By simulating real-world cyber attacks, organizations can evaluate their incident response plans and identify areas for improvement. This can help organizations respond more effectively to a real cyber attack and minimize the impact on their operations and reputation.

Modeling industry attacks is an important component of cyber risk management. By identifying potential threats and vulnerabilities and designing effective mitigations, organizations can reduce overall cyber risk and focus their efforts on what is most important. Modeling industry attacks also helps organizations prepare for potential cyber attacks and improve their incident response plans.

Attack Scenario

Modeling typical cyber attacks is a critical component of cyber risk management as it helps organizations identify potential vulnerabilities and develop effective mitigations to reduce the risk of a successful attack. Typical cyber attack models are designed to simulate common cyber attacks and provide insights into the tactics, techniques, and procedures used by attackers.

By modeling typical cyber attacks, organizations can identify potential vulnerabilities in their systems and networks and develop effective mitigations to reduce the risk of a successful attack. For example, suppose a typical cyber attack model reveals that phishing emails are commonly

used to access an organization's systems. In that case, the organization can prioritize implementing controls to prevent or detect phishing emails.

Modeling typical cyber attacks also helps organizations focus on mitigating risk for specific attacks of concern. Organizations can prioritize their risk management efforts and allocate resources effectively by understanding the tactics, techniques, and procedures used by attackers in typical cyber attacks. This can help organizations reduce the risk of a successful attack for specific attack types that concern them.

In addition, modeling typical cyber attacks can help organizations improve their incident response plans. By simulating common cyber attacks, organizations can evaluate their incident response plans and identify areas for improvement. This can help organizations respond more effectively to an actual cyber attack and minimize the impact on their operations and reputation.

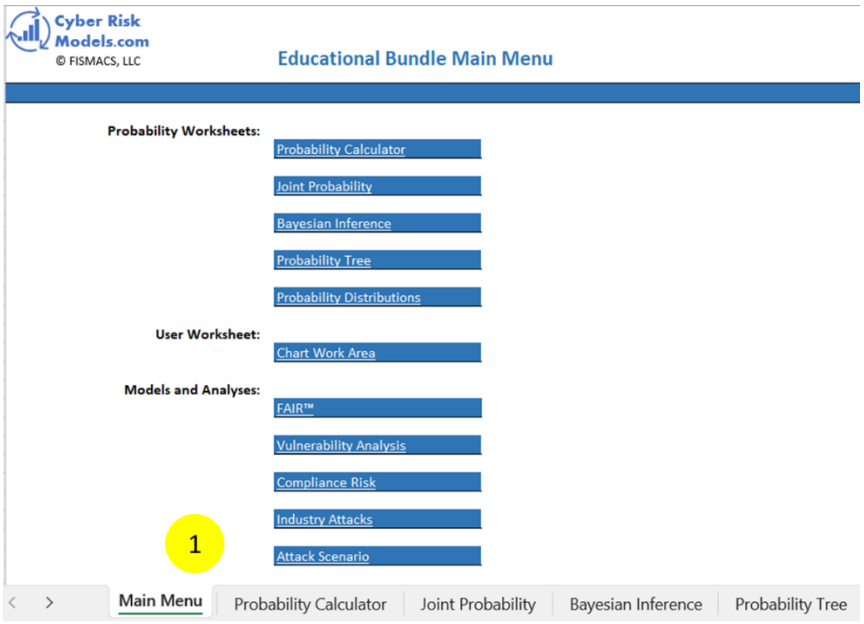
Modeling typical cyber attacks is a critical component of cyber risk management. By identifying potential vulnerabilities and developing effective mitigations, organizations can reduce the risk of a successful attack and focus their efforts on mitigating risk for specific attacks of concern. Modeling typical cyber attacks also helps organizations improve their incident response plans and prepare for potential cyber attacks.

USING THE MODELS

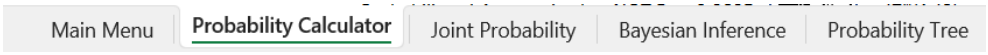
Navigation

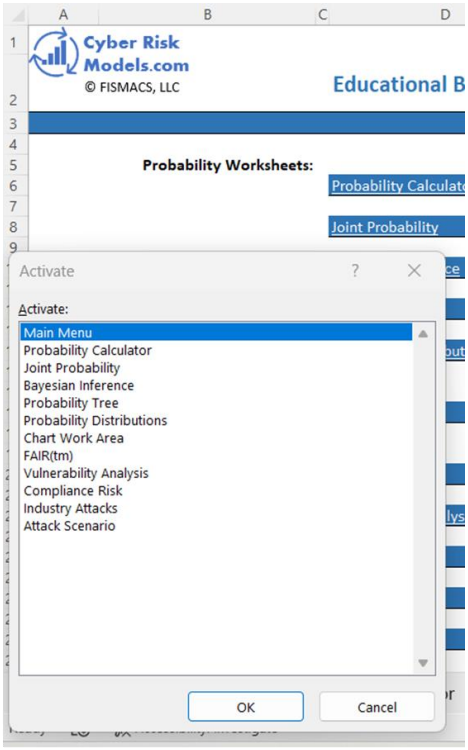
There are four ways to navigate between charts quickly:

1. Main Menu Navigation Buttons
2. Top Navigation Buttons
3. Excel Tabs
4. Excel Navigation Arrows (bottom-left) Right-Click Menu

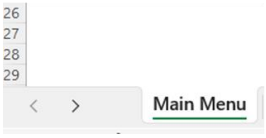


3


Main Menu
Probability Calculator
Joint Probability
Bayesian Inference
Probability Tree

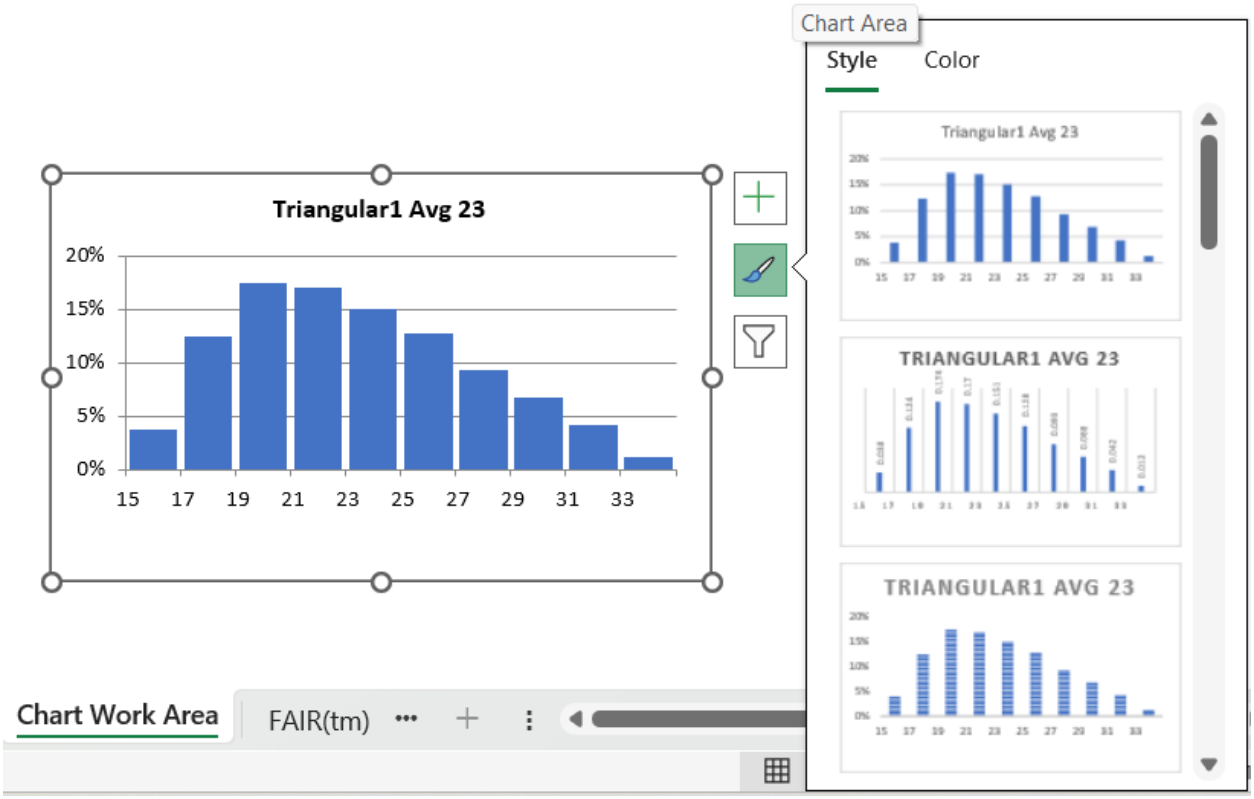

A
B
C
D
Cyber Risk Models.com
© FISMACS, LLC
Educational B
Probability Worksheets:
Probability Calculat
Joint Probability
Activate
Activate:
Main Menu
Probability Calculator
Joint Probability
Bayesian Inference
Probability Tree
Probability Distributions
Chart Work Area
FAIR(tm)
Vulnerability Analysis
Compliance Risk
Industry Attacks
Attack Scenario
OK
Cancel

4


26
27
28
29
Main Menu

Editing Charts

The models generate several probability distribution charts. To edit these, clip-and-copy them into the Chart Work Area tab. This allows you to always maintain the integrity of the original charts while allowing you to edit charts as needed.

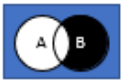
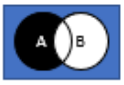
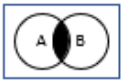
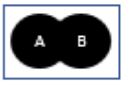
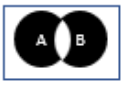
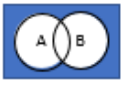
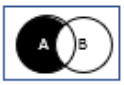
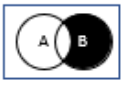


Probability Calculator

Steps:

- Input values A and B.
- Review calculations and select results.

Probability of two events	
P(A)	0.45
P(B)	0.15

Probability of A NOT occurring: P(~A)	0.55		=1-I7
Probability of B NOT occurring: P(~B)	0.85		=1-I8
Probability of A and B both occurring: P(A∩B):	0.0675		=I7*I8
Probability that A or B both occur: P(AUB)	0.5325		=I7+I8-I12
Probability that A or B occurs but NOT both: P(AΔB)	0.465		=I7+I8-2*(I12)
Probability of neither A nor B occurring: P(~(AUB))	0.4675		=1-I13
Probability of A occurring but NOT B:	0.3825		=I7*(1-I8)
Probability of B occurring but NOT A:	0.0825		=(1-I7)*I8

Notes:

Joint Probability

Steps

- Enter values A and B (Threat and Likelihood).
- Observe the calculation of joint probability.

Enter your estimates

	↓	A	~A
P(A)	0.200	**0.20**	**0.80**
P(B)	0.150	**0.15**	**0.85**
		0.35	1.65
		B	~B

1.42 <<- Odds of Event

This example requires A&B values

~ means not

∩ means union

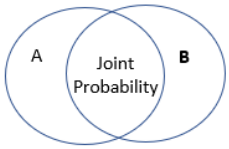
PR(A|B) is read "probability of A given that B occurs"

Joint Probability Matrix

	A↓	~A	SumB↓	
1 B→	0.030	0.120	0.150	←SumB
1 ~B	0.170	0.680	0.850	
2 SumA→	0.200	0.800	1.000	←Marginal
	SumA↑		↑Marginal	

Joint Probability 0.03

Pr(A∩B)	0.030
Pr(A|B)=Pr(A∩B)/Pr(B)	0.200
PR(B|A)=Pr(A∩B)/Pr(A)	0.150
Pr(A∩B)=Pr(A|B)*Pr(B)	0.030
Pr(A|B)=(Pr(B|A)*Pr(A))/Pr(B)	**0.200 <<--Bayesian's Formula**



Bayesian formulas are a way of describing a known universe. What is inside and not inside a set, and where they join for example.

Threat * Likelihood = Risk written another way is A*B which is the same as Pr(A∩B)=Pr(A|B)*Pr(B), or the joint probability where threat meets likelihood.

Bayes' Theorem:

- Expresses the relationship between Pr(A|B) and Pr(B|A).
- Expresses how a subjective degree of belief should rationally change to account for new evidence.

P(A) is the likelihood given the data P(B)

Notes:

Bayesian Inference

Steps:

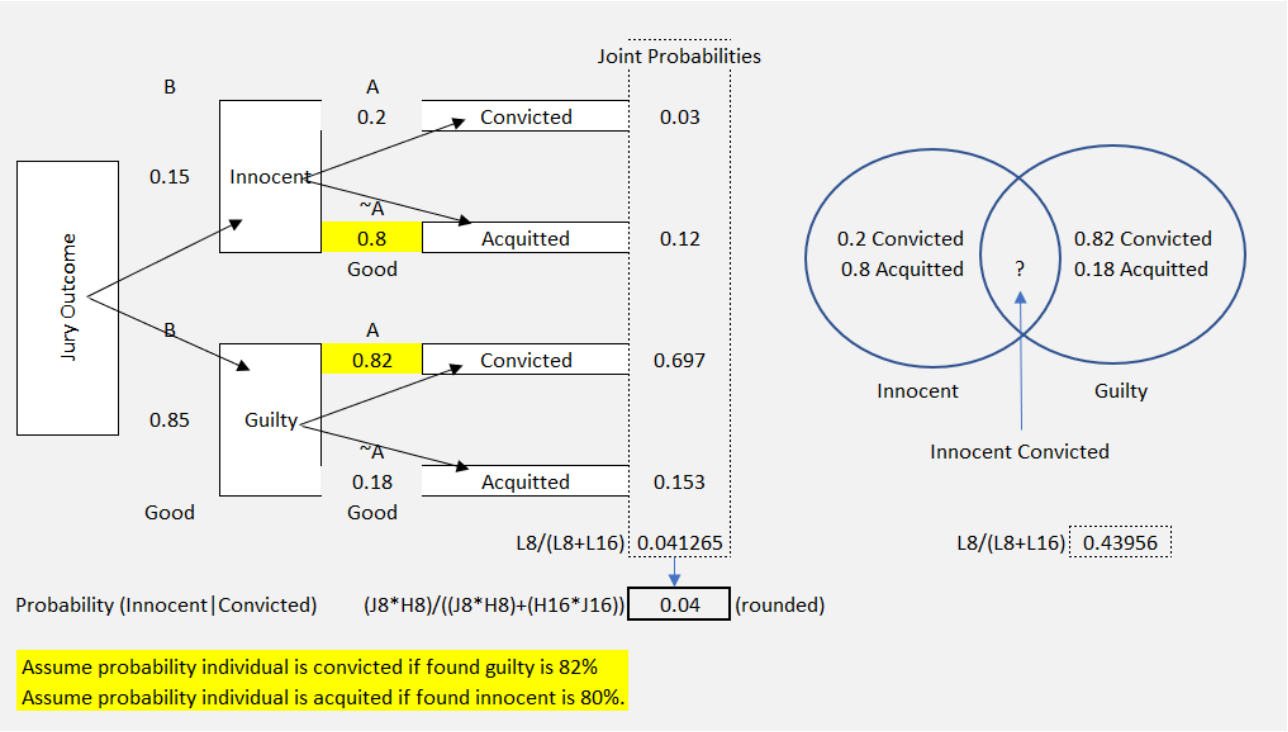
- Based on the data available, populate the Bayesian Box.
- Calculate the missing values to complete the Bayesian Box.
- Observe the Posterior value.
- Use Posterior value as the input for the next sequential Bayesian Box process. (Repeat as needed.)

Notes:

Probability Tree

Steps:

- Enter the text labels for the decision tree.
- Enter the known probability values.
- Calculate the missing probability values.
- Select the decision path and calculate the joint probabilities.
- Sum the joint probabilities of the decision path.



Notes:

Probability Distributions

Steps:

- Select the distribution(s) desired to perform your analysis.
- Enter meaningful labels for the desired probability (or be prepared to edit the associated chart title).
- Enter the distribution data.
- Update combined distribution formulas and allow the workbook to recalculate.
- Select and observe the resulting distribution charts.

	Triangular Distributions				
		Min	ML	Max	
#	Triangular1	5	20	35	22.2638
%	Triangular2	5%	20%	35%	0.1637
$	Triangular3	$2,500	$15,000	$50,000	24809

Combining Distributions	
Triangular1 * Triangular2	3.64458
Triangular1 * Triangular3	552344
Triangular2 * Triangular3	4061.22

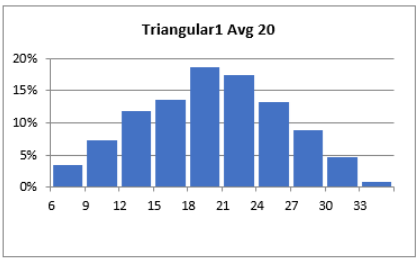
	Pert Distributions				
		Min	ML	Max	
#	Pert1	5	20	35	25.2302
%	Pert2	5%	20%	35%	0.17433
$	Pert3	$2,500	$15,000	$50,000	8202.92

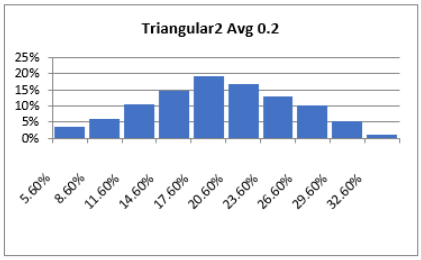
	Combining Distributions	
Pert1 * Pert2	4.39827	
Pert1 * Pert3	206961	
Pert2 * Pert3	1429.98	

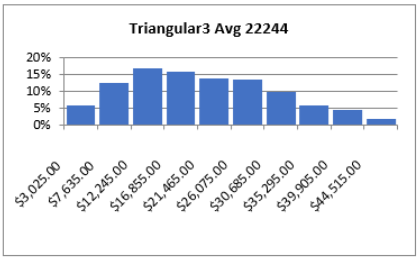
	Poisson Distributions	
	Rate	
Poisson1	4	3
Poisson2	5	5

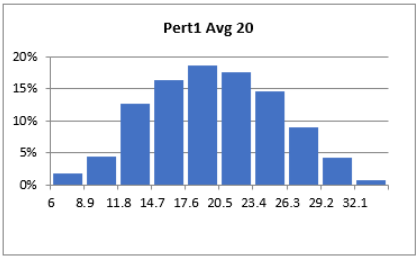
	Binomial Distributions		
	Trials #	Succes %	
Binom1	100	80%	83
Binom2	100	80%	83

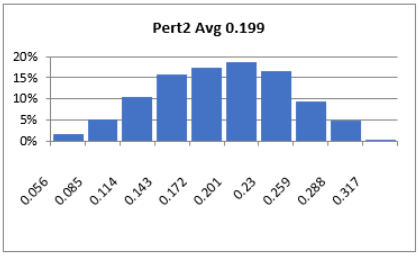
Notes:

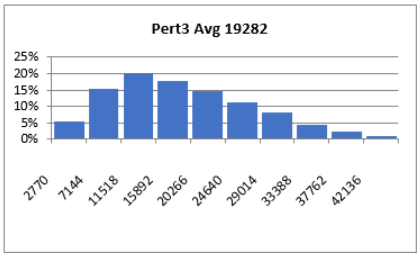

Triangular1 Avg 20
20%
15%
10%
5%
0%
6 9 12 15 18 21 24 27 30 33


Triangular2 Avg 0.2
25%
20%
15%
10%
5%
0%
5.60% 8.60% 11.60% 14.60% 17.60% 20.60% 23.60% 26.60% 29.60% 32.60%


Triangular3 Avg 22244
20%
15%
10%
5%
0%
$3,025.00 $7,635.00 $12,245.00 $16,855.00 $21,465.00 $26,075.00 $30,685.00 $35,295.00 $39,905.00 $44,515.00


Pert1 Avg 20
20%
15%
10%
5%
0%
6 8.9 11.8 14.7 17.6 20.5 23.4 26.3 29.2 32.1


Pert2 Avg 0.199
20%
15%
10%
5%
0%
0.056 0.085 0.114 0.143 0.172 0.201 0.23 0.259 0.288 0.317

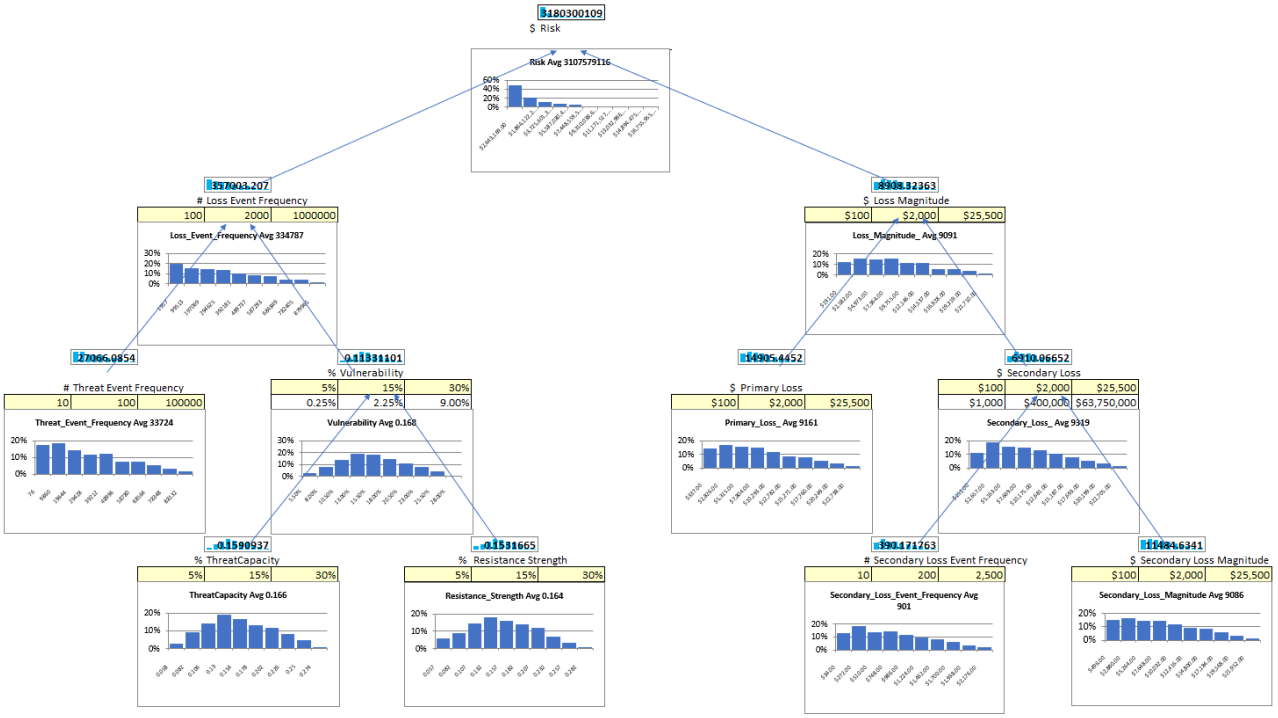

Pert3 Avg 19282
25%
20%
15%
10%
5%
0%
2770 7144 11518 15892 20266 24640 29014 33388 37762 42136

Notes:

FAIR

Steps:

- Enter *Resistance Strength* and *Threat Capacity* to generate *Vulnerability*. Enter the generated *Vulnerability* values or enter desired values.
- Enter *Threat Event Frequency* values.
- Enter *Secondary Loss Event Frequency* and *Secondary Loss Magnitude* values.
- Observe calculated *Secondary Loss*. Enter calculated *Secondary Loss* values or manually enter *Secondary Loss*.
- Enter *Primary Loss* values.
- Observe *Risk*.



Notes:

Vulnerability Analysis

Steps:

- Clip-and-copy vulnerability data as text.
- Manually inspect vulnerability data and select keywords.
- Enter keywords in column headers.
- Calculate statistics and observe results.

	MEDIUM	HIGH	CRITICAL
Microsoft	0	16	0
Ciso	0	0	0
DoS	6	12	0
unauthenticated	0	12	2
Internet Explorer	0	5	0
Office	0	6	0
Excel	0	3	0
MiTM	0	3	0
malicious user	0	11	0
exploit	6	26	2

Keyword Searching and Basic Formulas

ID No	Vulnerability Description	Severity	# Findings	Microsoft	Ciso	DoS	unauthenticated	Internet Explorer	Office	Excel	MiTM	malicious user	exploit	Results
CVE-2018-0094	A vulnerability in IPv6 ingress packet processing for C	HIGH	1			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0211	A vulnerability in specific CLI commands for the Cisco	MEDIUM	1			DoS							exploit	DoS, exploit
CVE-2018-0094	A vulnerability in IPv6 ingress packet processing for C	HIGH	1			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0095	A vulnerability in IPv6 ingress packet processing for C	HIGH	2			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0096	A vulnerability in IPv6 ingress packet processing for C	HIGH	3			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0097	A vulnerability in IPv6 ingress packet processing for C	HIGH	4			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0098	A vulnerability in IPv6 ingress packet processing for C	HIGH	5			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0099	A vulnerability in IPv6 ingress packet processing for C	HIGH	6			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0019	A malicious user with unrestricted access to the AppF	HIGH	5									alicious us	exploit	malicious user, exploit
CVE-2018-0020	A malicious user with unrestricted access to the AppF	HIGH	6									alicious us	exploit	malicious user, exploit
CVE-2018-0211	A vulnerability in specific CLI commands for the Cisco	MEDIUM	2			DoS							exploit	DoS, exploit
CVE-2018-0772	Internet Explorer in Microsoft Windows 7 SP1, Windo	HIGH	1	Microsoft				rnet Explo						Microsoft, Internet Explorer
CVE-2018-0773	Microsoft Edge in Windows 10 1709 allows an attack	HIGH	1	Microsoft										Microsoft
CVE-2018-0105	A vulnerability in IPv6 ingress packet processing for C	HIGH	12			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0106	A vulnerability in IPv6 ingress packet processing for C	HIGH	13			DoS	authentica						exploit	DoS, unauthenticated, exploit
CVE-2018-0107	A vulnerability in IPv6 ingress packet processing for C	HIGH	14			DoS	authentica						exploit	DoS, unauthenticated, exploit

Notes:

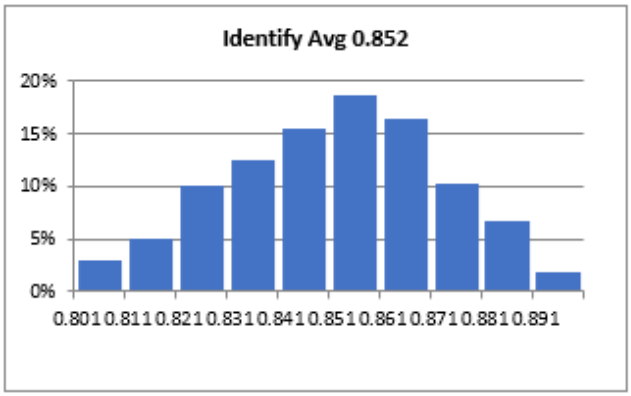
Compliance Risk

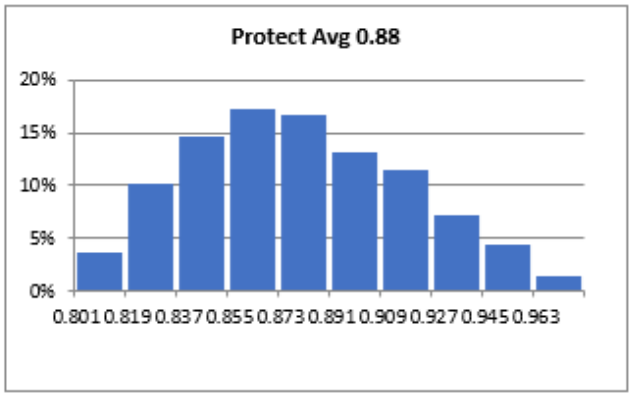
Steps:

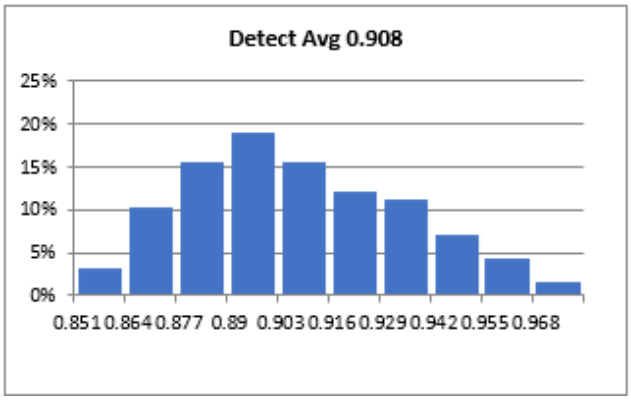
- Estimate % complete for each compliance item.
- Observe estimated probabilities for each compliance category.
- Select and copy desired charts into *Chart Work Area* to edit as desired.

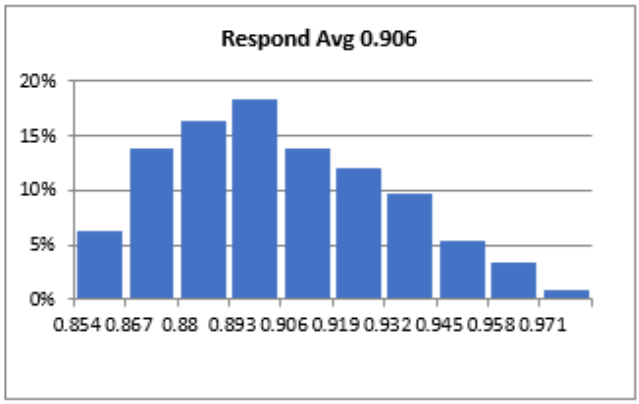
		Min	ML	Max
0.831461113	Identify	80.00%	85.83%	90.00%
0.912607481	Protect	80.00%	86.33%	98.00%
0.904710442	Detect	85.00%	89.33%	98.00%
0.893147343	Respond	85.00%	88.60%	98.00%
0.887008244	Recovery	85.00%	89.33%	98.00%

Est %	Category	Identify	Protect	Detect	Respond	Recovery
85.00%	Asset Management	X				
85.00%	Business Environment	X				
85.00%	Governance	X				
90.00%	Risk Assessment	X				
90.00%	Risk Management	X				
80.00%	Supply Chain Risk Management	X				
85.00%	Identify Management		X			
98.00%	Awareness & Training		X			
85.00%	Data Security		X			
80.00%	Information Protection Processes		X			
85.00%	Maintenance		X			
85.00%	Protective Technology		X			
85.00%	Anomalies & Events			X		
98.00%	Security Continuous Monitoring			X		
85.00%	Detection Process			X		
85.00%	Response Planning				X	
85.00%	Communications				X	
98.00%	Analysis				X	
90.00%	Mitigation				X	
85.00%	Improvement				X	
85.00%	Recovery Planning					X
98.00%	Improvement					X
85.00%	Communications					X
87.48%	**<<--Complete**					


Identify Avg 0.852
20%
15%
10%
5%
0%
0.801 0.811 0.821 0.831 0.841 0.851 0.861 0.871 0.881 0.891


Protect Avg 0.88
20%
15%
10%
5%
0%
0.801 0.819 0.837 0.855 0.873 0.891 0.909 0.927 0.945 0.963


Detect Avg 0.908
25%
20%
15%
10%
5%
0%
0.851 0.864 0.877 0.89 0.903 0.916 0.929 0.942 0.955 0.968


Respond Avg 0.906
20%
15%
10%
5%
0%
0.854 0.867 0.88 0.893 0.906 0.919 0.932 0.945 0.958 0.971

Notes:

Industry Attacks

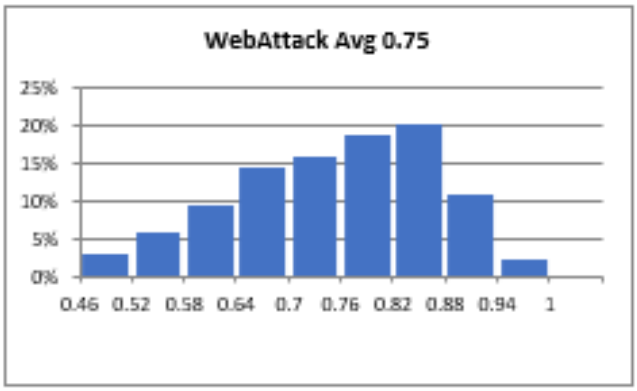
Steps:

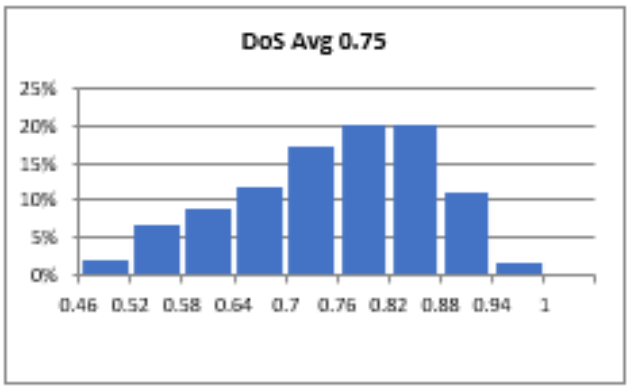
- Enter an estimate of strength for each mitigation area.
- Observe calculated distributions for each attack category.
- Select and copy desired charts into *Chart Work Area* to edit as desired.

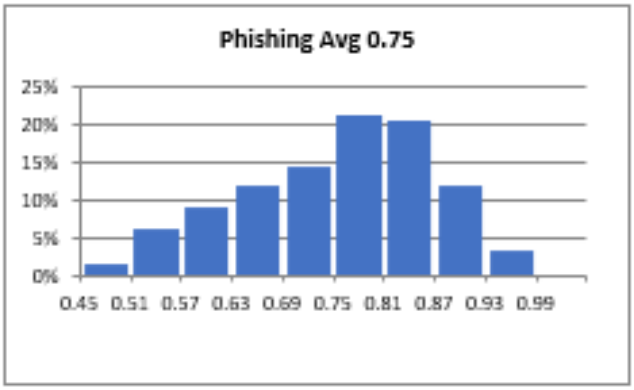
		Min	ML	Max
0.795253271	WebAttack	45.00%	83.69%	98.00%
0.766472163	DoS	45.00%	83.30%	98.00%
0.748975196	Phishing	45.00%	84.00%	98.00%
0.731009199	Malware	45.00%	84.17%	98.00%
0.848288232	3rd-Party	80.00%	85.48%	98.00%
0.911380248	Mobile	80.00%	86.41%	98.00%

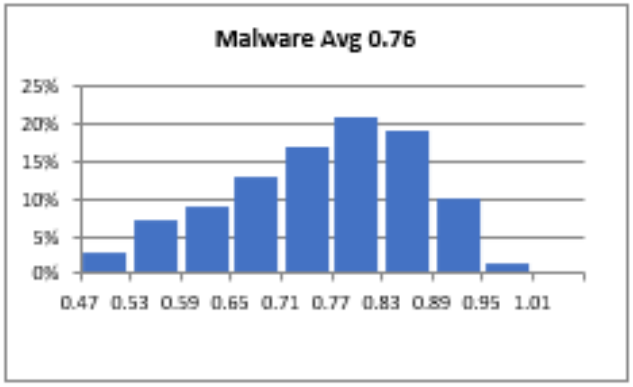
Est	Mitigations	WebAttacl	DoS	Phishing	Malware	3rd-Party	Mobile
85.00%	Cyber Awareness Training			X	X		X
98.00%	Security Policies & Procedures	X	X	X	X	X	X
45.00%	Network Administration Procedures	X	X	X	X		
90.00%	Insider Threat Program						
90.00%	Contractual Clauses					X	X
80.00%	Data Loss Prevention					X	X
85.00%	Encryption					X	X
98.00%	Identification & Authentication			X		X	X
85.00%	Least Privileges	X	X	X	X	X	X
80.00%	Multi-Factor Authentication					X	X
85.00%	Perimeter Defense Firewalls	X	X	X	X	X	
85.00%	Intrusion Detection Systems	X	X	X	X	X	X
85.00%	Malware Enterprise Defense	X	X	X	X	X	X
98.00%	Web Filtering	X	X		X		X
85.00%	Email Filtering and Blocking			X	X		X
85.00%	Segmentation	X	X	X	X	X	X
85.00%	Sensitive Data Protection Plan					X	X

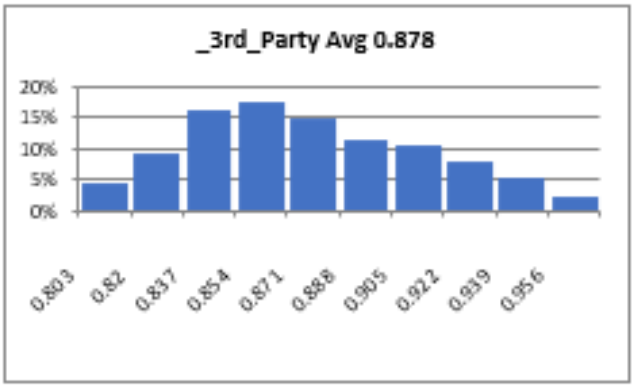
Notes:

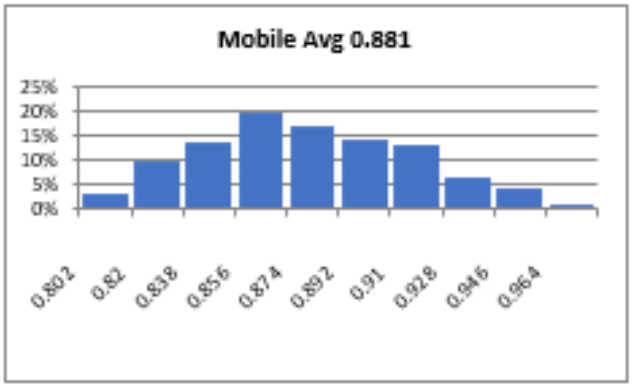

WebAttack Avg 0.75
25%
20%
15%
10%
5%
0%
0.46 0.52 0.58 0.64 0.7 0.76 0.82 0.88 0.94 1


DoS Avg 0.75
25%
20%
15%
10%
5%
0%
0.46 0.52 0.58 0.64 0.7 0.76 0.82 0.88 0.94 1


Phishing Avg 0.75
25%
20%
15%
10%
5%
0%
0.45 0.51 0.57 0.63 0.69 0.75 0.81 0.87 0.93 0.99


Malware Avg 0.76
25%
20%
15%
10%
5%
0%
0.47 0.53 0.59 0.65 0.71 0.77 0.83 0.89 0.95 1.01


_3rd_Party Avg 0.878
20%
15%
10%
5%
0%
0.803 0.82 0.837 0.854 0.871 0.888 0.905 0.922 0.939 0.956

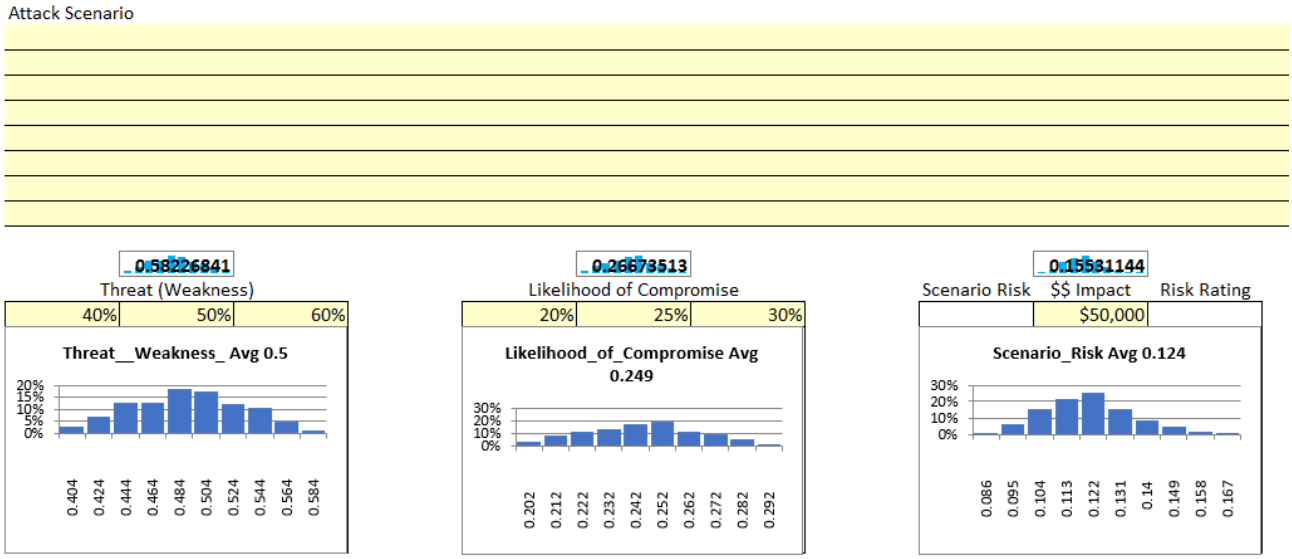

Mobile Avg 0.881
25%
20%
15%
10%
5%
0%
0.802 0.82 0.838 0.856 0.874 0.892 0.91 0.928 0.946 0.964

Notes:

Attack Scenario

Steps:

- Enter the *Attack Scenario* description.
- Enter values for *Impact Scale*.
- Enter *Threat* values.
- Enter *Likelihood* values.
- Enter the *Estimated Impact* value.
- Observe calculated risks and distributions.
- Select and copy desired charts into *Chart Work Area* to make edits.



Notes:

EXPLORING PROBABILITY

Probability Calculator Formulas Explained

Probability of A NOT Occurring: P(~A)

This equation represents the likelihood of an event A not happening. In probability theory, the complement of an event A is the set of all outcomes that are not in A. The complement of A is denoted as ~A, and it represents the event that A does not occur.

The probability of A not occurring, represented as P(~A), is calculated by subtracting the probability of A from 1. In other words, P(~A) = 1 - P(A). This is because the probability of either A happening or not happening is always equal to 1. Therefore, if we know the probability of A happening, we can easily calculate the probability of A not happening by subtracting it from 1.

The concept of the complement of an event is important in probability theory because it allows us to calculate the probability of complex events. For example, if we want to calculate the probability of either A or B happening, we can use the formula P(A or B) = P(A) + P(B) - P(A and B). However, if we only know the probability of A happening, we can use the complement of A to calculate the probability of B happening. Specifically, P(B) = 1 - P(~B), where ~B represents the complement of B.

In real-world applications, the concept of the complement of an event is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a stock price going up can be used to calculate the probability of the stock price going down. In engineering, the probability of a component failing can be used to calculate the probability of the component not failing. In healthcare, the probability of a patient having a disease can be used to calculate the probability of the patient not having the disease.

The equation “Probability of A NOT occurring: P(~A” represents the likelihood of an event A not happening. It is calculated by subtracting the probability of A from 1 and is an important concept in probability theory that allows us to calculate the probability of complex events.

Probability of B NOT Occurring: P(~B)

The equation “Probability of B NOT occurring: P(~B” represents the likelihood of an event B not happening. In probability theory, the complement of an event B is the set of all outcomes that are not in B. The complement of B is denoted as ~B, and it represents the event that B does not occur.

The probability of B not occurring, represented as P(~B), is calculated by subtracting the probability of B from 1. In other words, P(~B) = 1 - P(B). This is because the probability of either B happening or not happening is always equal to 1. Therefore, if we know the probability of B happening, we can easily calculate the probability of B not happening by subtracting it from 1.

The concept of the complement of an event is important in probability theory because it allows us to calculate the probability of complex events. For example, if we want to calculate the probability of either A or B happening, we can use the formula P(A or B) = P(A) + P(B) - P(A and B). However, if we only know the probability of B happening, we can use the complement of B to calculate the probability of A happening. Specifically, P(A) = 1 - P(~A), where ~A represents the complement of A.

In real-world applications, the concept of the complement of an event is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a stock price going down can be used to calculate the probability of the stock price going up. In engineering, the probability of a component not failing can be used to calculate the probability of the component failing. In healthcare, the probability of a patient not having a disease can be used to calculate the probability of the patient having the disease.

The equation “Probability of B NOT occurring: P(~B” represents the likelihood of an event B not happening. It is calculated by subtracting the probability of B from 1 and is an important concept in probability theory that allows us to calculate the probability of complex events.

Probability of A and B Both Occurring: P(A∩B)

The equation “Probability of A and B both occurring: P(A∩B” represents the likelihood of two events, A and B, happening together. In probability theory, the intersection of two events A and B is the set of all outcomes that are in both A and B. The intersection of A and B is denoted as A∩B, and it represents the event that A and B both occur.

The probability of A and B both occurring, represented as P(A∩B), is calculated by multiplying the probability of A by the probability of B given that A has occurred. In other words, P(A∩B) = P(A) * P(B|A). This is because the probability of A and B both occurring is equal to the probability of A occurring multiplied by the probability of B occurring given that A has occurred.

The concept of the intersection of two events is important in probability theory because it allows us to calculate the probability of complex events. For example, if we want to calculate the probability of either A or B happening, we can use the formula P(A or B) = P(A) + P(B) - P(A∩B). However, if we know the probability of A and B both occurring, we can use this information to calculate the probability of other events, such as the probability of A occurring

given that B has occurred. Specifically, P(A|B) = P(A∩B) / P(B), where P(A|B) represents the probability of A occurring given that B has occurred.

In real-world applications, the concept of the intersection of two events is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a stock price going up and the probability of a company reporting positive earnings can be used to calculate the probability of the stock price going up and the company reporting positive earnings. In engineering, the probability of two components failing together can be used to calculate the overall reliability of a system. In healthcare, the probability of a patient having two risk factors can be used to identify patients who are at higher risk for certain diseases.

The equation "Probability of A and B both occurring: P(A∩B" represents the likelihood of two events, A and B, happening together. It is calculated by multiplying the probability of A by the probability of B given that A has occurred and is an important concept in probability theory that allows us to calculate the probability of complex events.

In cyber security, we will use this equation, this joint probability, to calculate risk. In this case, we are calculating threat times likelihood. Threat is the weakness in our systems or controls. Likelihood is the likelihood that a threat actor could leverage these threats against us, culminating in a cyber attack or data breach. Threat without likelihood is not risk.

Probability that A or B Both Occur: P(AUB)

The equation "Probability that A or B both occur: P(AUB" represents the likelihood of two events, A and B, happening together or separately. In probability theory, the union of two events A and B is the set of all outcomes that are in either A or B or both. The union of A and B is denoted as AUB, and it represents the event that A or B or both occur.

The probability of A or B both occurring, represented as P(AUB), is calculated by adding the probability of A to the probability of B and then subtracting the probability of both A and B occurring together. In other words, P(AUB) = P(A) + P(B) - P(A and B). This is because the probability of either A or B happening or both happening is equal to the sum of the probabilities of A and B minus the probability of both A and B occurring together.

The concept of the union of two events is important in probability theory because it allows us to calculate the probability of complex events. For example, if we want to calculate the probability of A happening or B happening, we can use the formula P(A or B) = P(A) + P(B) - P(A and B). This formula is also known as the addition rule of probability. Additionally, if we know the probability of A or B both occurring, we can use this information to calculate the probability of other events, such as the probability of A occurring given that B has occurred. Specifically, P(A|B) =

P(A and B) / P(B), where P(A|B) represents the probability of A occurring given that B has occurred.

In real-world applications, the concept of the union of two events is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a stock price going up or a company reporting positive earnings can be used to calculate the probability of the stock price going up or the company reporting positive earnings. In engineering, the probability of two components failing together or separately can be used to calculate the overall reliability of a system. In healthcare, the probability of a patient having two symptoms can be used to identify patients who are at higher risk for certain diseases.

The equation “Probability that A or B both occur: P(AUB” represents the likelihood of two events, A and B, happening together or separately. It is calculated by adding the probability of A to the probability of B and then subtracting the probability of both A and B occurring together and is an important concept in probability theory that allows us to calculate the probability of complex events.

Probability that A or B Occurs but NOT Both: P(AΔB)

The equation “Probability that A or B occurs but NOT both: P(AΔB” represents the likelihood of either event A or event B happening, but not both happening simultaneously. In probability theory, the symmetric difference of two events A and B is the set of all outcomes that are in either A or B, but not in both. The symmetric difference of A and B is denoted as AΔB, and it represents the event that A or B occurs but not both.

The probability of A or B occurring but not both, represented as P(AΔB), is calculated by adding the probability of A to the probability of B and then subtracting twice the probability of both A and B occurring together. In other words, P(AΔB) = P(A) + P(B) - 2P(A and B). This is because we want to include the probabilities of A and B happening separately, but we need to subtract the probability of both A and B happening together to avoid double counting.

The concept of the symmetric difference of two events is important in probability theory because it allows us to calculate the probability of mutually exclusive events. For example, if we want to calculate the probability of either A or B happening, but not both, we can use the formula P(AΔB) = P(A) + P(B) - 2P(A and B). This formula is also known as the inclusion-exclusion principle. Additionally, if we know the probability of A or B occurring but not both, we can use this information to calculate the probability of other events, such as the probability of A occurring given that B has not occurred. Specifically, P(A|~B) = P(A and ~B) / P(~B), where P(A|~B) represents the probability of A occurring given that B has not occurred.

In real-world applications, the concept of the symmetric difference of two events is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a stock price going up or going down can be used to calculate the probability of the stock price staying the same. In engineering, the probability of two components failing separately can be used to calculate the overall reliability of a system. In healthcare, the probability of a patient having one symptom but not another can be used to identify patients who are at higher risk for certain diseases.

The equation “Probability that A or B occurs but NOT both: P(AΔB” represents the likelihood of either event A or event B happening, but not both happening simultaneously. It is calculated by adding the probability of A to the probability of B and then subtracting twice the probability of both A and B occurring together and is an important concept in probability theory that allows us to calculate the probability of mutually exclusive events.

Probability of Neither A nor B Occurring: P(~(AUB))

The equation “Probability of neither A nor B occurring: P(~(AUB)” represents the likelihood of neither event A nor event B happening. In probability theory, the complement of an event A is the set of all outcomes that are not in A. The complement of A is denoted as ~A, and it represents the event that A does not occur. Similarly, the complement of the union of two events A and B is the set of all outcomes that are not in either A or B or both. The complement of AUB is denoted as ~(AUB), and it represents the event that neither A nor B occurs.

The probability of neither A nor B occurring, represented as P(AUB)) = (1 - P(A)) x (1 - P(B)). This is because we want to find the probability that neither A nor B occurs, which is the complement of AUB. We can find this probability by finding the probability of A not occurring and the probability of B not occurring and then multiplying them together.

The concept of the complement of an event is important in probability theory because it allows us to calculate the probability of events that are difficult to calculate directly. For example, if we want to calculate the probability of neither A nor B occurring, we can use the formula P(~(AUB)) = (1 - P(A)) x (1 - P(B)). This formula is also known as the multiplication rule of probability. Additionally, if we know the probability of neither A nor B occurring, we can use this information to calculate the probability of other events, such as the probability of A occurring given that B has not occurred. Specifically, P(A|~B) = P(A and ~B) / P(~B), where P(A|~B) represents the probability of A occurring given that B has not occurred.

In real-world applications, the concept of the complement of an event is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a stock price going up or going down can be used to calculate the probability of the stock price

staying the same. In engineering, the probability of a system failing can be used to calculate the probability of the system functioning properly. In healthcare, the probability of a patient not having a certain disease can be used to identify patients who are at lower risk for that disease.

The equation “Probability of neither A nor B occurring: P(~(AUB)” represents the likelihood of neither event A nor event B happening. It is calculated by subtracting the probability of A from 1 and then multiplying it by the probability of B from 1 and is an important concept in probability theory that allows us to calculate the probability of events that are difficult to calculate directly.

Probability of A Occurring but NOT B

The equation “Probability of A occurring but NOT ” represents the likelihood of event A happening but event B not happening. In probability theory, the difference between two events, A and B, is the set of all outcomes in A but not B. The difference between A and B is denoted as A-B, representing the event that A occurs, but B does not.

The probability of A occurring but not B, represented as P(A-B), is calculated by subtracting the probability of both A and B occurring together from the probability of A occurring. In other words, P(A-B) = P(A) - P(A and B). This is because we want to find the probability of A occurring but not B, which is the difference between A and B. We can find this probability by finding the probability of A occurring and then subtracting the probability of both A and B occurring together to avoid double counting.

The concept of the difference of two events is important in probability theory because it allows us to calculate the probability of events that are not mutually exclusive. For example, if we want to calculate the probability of A occurring but not B, we can use the formula P(A-B) = P(A) - P(A and B). This formula is also known as the subtraction rule of probability. Additionally, if we know the probability of A occurring but not B, we can use this information to calculate the probability of other events, such as the probability of B occurring given that A has occurred. Specifically, P(B|A) = P(B and A) / P(A), where P(B|A) represents the probability of B occurring given that A has occurred.

In real-world applications, the concept of the difference of two events is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a stock price going up or down can be used to calculate the probability of a certain investment strategy being successful. In engineering, the probability of two components failing separately can be used to calculate the overall reliability of a system. In healthcare, the probability of a patient having one symptom but not another can be used to identify patients who are at higher risk for certain diseases.

The equation “Probability of A occurring but NOT ” represents the likelihood of event A happening but event B not happening. It is calculated by subtracting the probability of both A and B occurring together from the probability of A occurring. It is an important concept in probability theory that allows us to calculate the probability of events that are not mutually exclusive.

Probability of B Occurring but NOT A

The equation “Probability of B occurring but NOT ” represents the likelihood of event B happening but event A not happening. In probability theory, the difference between two events, A and B, is the set of all outcomes in B but not in A. The difference between B and A is denoted as B-A, representing the event that B occurs but A does not.

The probability of B occurring but not A, represented as P(B-A), is calculated by subtracting the probability of both A and B occurring together from the probability of B occurring. In other words, P(B-A) = P(B) - P(A and B). This is because we want to find the probability of B occurring but not A, which is the difference between B and A. We can find this probability by finding the probability of B occurring and then subtracting the probability of both A and B occurring together to avoid double counting.

The concept of the difference of two events is important in probability theory because it allows us to calculate the probability of events that are not mutually exclusive. For example, if we want to calculate the probability of B occurring but not A, we can use the formula P(B-A) = P(B) - P(A and B). This formula is also known as the subtraction rule of probability. Additionally, if we know the probability of B occurring but not A, we can use this information to calculate the probability of other events, such as the probability of A occurring given that B has occurred. Specifically, P(A|B) = P(A and B) / P(B), where P(A|B) represents the probability of A occurring given that B has occurred.

In real-world applications, the concept of the difference of two events is used in many fields, including finance, engineering, and healthcare. For example, in finance, the probability of a certain investment strategy being successful can be calculated by considering the probability of different market conditions. In engineering, the probability of a system functioning properly when certain components are present can be calculated by considering the probability of different failure modes. In healthcare, the probability of a patient having one symptom but not another can be used to identify patients who are at higher risk for certain diseases.

The equation “Probability of B occurring but NOT ” represents the likelihood of event B happening but event A not happening. It is calculated by subtracting the probability of both A and B occurring together from the probability of B occurring. It is an important concept in

probability theory that allows us to calculate the probability of events that are not mutually exclusive.

Joint Probability Explained

Joint probability is a concept in probability theory that represents the likelihood of two or more events occurring together. It is denoted as P(A ∩ B), where A and B are two events. Joint probability is an important concept in probability theory because it allows us to calculate the probability of events that are not independent.

The joint probability of two events A and B can be calculated by multiplying the probability of A by the probability of B given that A has occurred. In other words, P(A ∩ B) = P(A) x P(B|A). This formula is known as the multiplication rule of probability. The probability of B given that A has occurred is known as the conditional probability of B given A and is denoted as P(B|A). Conditional probability is the probability of an event occurring given that another event has occurred.

For example, suppose we are flipping two coins. The probability of getting heads on the first coin is 1/2, and the probability of getting heads on the second coin is also 1/2. The joint probability of getting heads on both coins is P(A ∩ B) = P(A) x P(B|A) = (1/2) x (1/2) = 1/4. This means that the probability of getting heads on both coins is 1/4 or 25%.

Joint probability can also be extended to more than two events. For example, suppose we are rolling three dice. The probability of getting a 1 on the first die is 1/6, the probability of getting a 2 on the second die given that a 1 has been rolled on the first die is also 1/6, and the probability of getting a 3 on the third die given that a 1 has been rolled on the first die and a 2 has been rolled on the second die is also 1/6. The joint probability of getting a 1 on the first die, a 2 on the second die, and a 3 on the third die is P(A ∩ B ∩ C) = P(A) x P(B|A) x P(C|A and B) = (1/6) x (1/6) x (1/6) = 1/216. This means that the probability of getting a 1 on the first die, a 2 on the second die, and a 3 on the third die is 1/216 or 0.46%.

Joint probability is used in many real-world applications, including finance, engineering, and healthcare. In finance, joint probability can be used to calculate the probability of certain market conditions occurring together. For example, the joint probability of the stock market going up and interest rates going down can be used to evaluate the risk of a certain investment strategy. In engineering, joint probability can be used to calculate the probability of multiple components failing together. For example, the joint probability of a power supply failing and a cooling system failing can be used to evaluate the reliability of a computer system. In healthcare, joint probability can be used to evaluate the risk of multiple diseases occurring

together. For example, the joint probability of a patient having high blood pressure and high cholesterol can be used to identify patients who are at higher risk for heart disease.

Joint probability is a concept in probability theory that represents the likelihood of two or more events occurring together. It is calculated by multiplying the probability of one event by the conditional probability of the other event given that the first event has occurred. Joint probability is an important concept in probability theory because it allows us to calculate the probability of events that are not independent. Joint probability is used in many real-world applications, including finance, engineering, and healthcare.

Bayesian Inference

Bayesian inference is a statistical method that allows us to update our beliefs about the probability of an event occurring based on new evidence or information. It is named after the 18th-century mathematician and philosopher Thomas Bayes, who first proposed the idea of using probability to reason about uncertain events.

The basic idea behind Bayesian inference is to use prior knowledge or beliefs about the probability of an event occurring and then update these beliefs based on new evidence or information. This is done by using the Bayes Theorem, which relates the probability of an event occurring to the probability of observing certain evidence or data.

Bayes' Theorem states that the probability of an event A given evidence B is equal to the probability of observing evidence B given that event A has occurred, multiplied by the prior probability of event A, divided by the probability of observing evidence B. Mathematically, this can be written as:

$P(A|B) = P(B|A) \times P(A) / P(B)$

Where $P(A|B)$ is the posterior probability of event A given evidence B, $P(B|A)$ is the likelihood of observing evidence B given that event A has occurred, $P(A)$ is the prior probability of event A, and $P(B)$ is the probability of observing evidence B.

To use Bayesian inference, we start with a prior probability distribution that represents our initial beliefs about the probability of an event occurring. We then update this distribution based on new data or evidence, using Bayes' Theorem to calculate the posterior probability distribution.

For example, suppose we are trying to estimate the probability that a coin is biased towards heads. Our prior belief is that the coin is fair, so we assign a prior probability of 0.5 to the event

that the coin lands heads. We then flip the coin 10 times and observe that it lands heads 8 times. We can use Bayesian inference to update our belief about the probability of the coin being biased towards heads.

Given the observed data, we can use Bayes' Theorem to calculate the posterior probability of the coin being biased toward heads. This involves multiplying the prior probability by the likelihood of observing the data, given the hypothesis that the coin is biased towards heads, and then normalizing by the probability of observing the data. In this case, the posterior probability of the coin being biased towards heads is 0.97, indicating strong evidence favoring the hypothesis.

Bayesian inference is a powerful statistical method that allows us to update our beliefs about the probability of an event occurring based on new evidence or information. It involves using Bayes' Theorem to calculate the posterior probability distribution, which represents our updated beliefs about the probability of the event. Bayesian inference is widely used in fields such as machine learning, artificial intelligence, and data science and is an essential tool for anyone working with uncertain or probabilistic data.

Probability Tree

Probability trees, or decision trees, are a valuable tool for quantifying cybersecurity risks. They allow us to model complex decision-making processes and calculate the probabilities of different outcomes based on the likelihood of various events occurring. We will explore the concepts and layouts related to probability trees used for cybersecurity risk quantification.

Concepts

The basic concept behind a probability tree is to break down a complex decision or event into its parts and assign probabilities to each outcome. This is done by creating a series of branches representing the different possible outcomes of a decision or event. Each branch is assigned a probability based on the likelihood of that outcome occurring.

For example, let's say we are trying to quantify the risk of a cyber attack on a company's network. We can use a probability tree to model the attack's different possible outcomes and calculate each outcome's probabilities. The branches of the tree might include:

- The attacker gains access to the network
- The company's security measures block the attacker.
- The attacker gains access to some but not all of the network

Each branch would be assigned a probability based on the likelihood of that outcome occurring. For example, the probability of the attacker gaining access to the network might be higher if the company's security measures are weak or outdated.

Layout

The layout of a probability tree consists of a series of branches that represent the different possible outcomes of a decision or event. Each branch is assigned a probability based on the likelihood of that outcome occurring. The branches then split into further branches, representing the different possible outcomes of subsequent decisions or events.

The layout of a probability tree can be simple or complex, depending on the decision or event being modeled. For example, a simple probability tree might consist of just a few branches, whereas a complex probability tree might consist of dozens or even hundreds of branches.

In the context of cybersecurity risk quantification, a probability tree might look something like this:

```
Start
|
|--- Attacker gains access to the network (P1)
|     |
|     |--- Data breach occurs (P2)
|     |
|     |--- No data breach occurs (1 - P2)
|
|--- Attacker is blocked by security measures (1 - P1)
      |
      |--- No data breach occurs (P3)
      |
      |--- Data breach occurs (1 - P3)
```

In this example, the probability tree models the risk of a cyber attack on the company's network. The tree starts with the decision of whether or not the attacker gains access to the network. If the attacker does gain access, there is a probability of a data breach occurring (P2). If security measures block the attacker, there is a probability of no data breach occurring (P3).

Calculating Probabilities

Once the probability tree has been constructed, we can use it to calculate the probabilities of different outcomes. This is done by multiplying the probabilities along each branch of the tree. For example, if the probability of the attacker gaining access to the network is P1 and the probability of a data breach occurring is P2, the overall probability of a data breach occurring would be P1 * P2.

In cybersecurity risk quantification, probabilities might be assigned based on historical data, expert opinions, or statistical modeling. For example, the probability of an attacker gaining access to the network might be based on the likelihood of a known vulnerability being exploited, whereas the probability of a data breach occurring might be based on the likelihood of sensitive data being present on the network.

Expected Value

In addition to calculating probabilities, probability trees can also be used to calculate the expected value of different decisions. The expected value is the sum of the probability of each outcome multiplied by its associated payoff. In cybersecurity risk quantification, the payoff might represent the financial cost of a data breach or the reputation damage caused by a cyber attack.

For example, let's say the expected value of a data breach is $1 million, and the probability of a data breach occurring is 0.1. The expected value of the data breach would be $1 million * 0.1 = $100,000. This expected value can then be used to inform decisions about cybersecurity investments, such as whether to invest in

Probability Distributions

Probability distributions are mathematical functions that describe the likelihood of different outcomes in a random event. They are used extensively in various fields, including finance, engineering, and science, to model and analyze data. In risk management, probability distributions quantify the likelihood of risks and their potential impact on an organization. We will discuss four probability distributions – Poisson, Triangular, PERT, and Bernoulli – and their use in quantifying risk with simple examples.

Poisson Distribution

The Poisson distribution is a discrete probability distribution that models the number of events that occur in a fixed interval of time or space. It is commonly used to model rare events that

occur randomly, such as accidents or equipment failures. The Poisson distribution is characterized by a single parameter, λ, which represents the average number of events that occur in the interval.

For example, a company that operates a fleet of trucks may use the Poisson distribution to model the number of accidents that occur per month. Suppose the company experiences an average of 5 accidents per month. In that case, the Poisson distribution can be used to calculate the probability of experiencing a certain number of accidents in a given time period. This information can be used to estimate the likelihood of an accident and to develop appropriate risk management strategies.

The Poisson distribution is also used to model the number of defects in a manufacturing process. If a factory produces widgets, for example, with an average of 5% defects per widget, then it can be modeled using the Poisson distribution. The probability that the factory will produce 100 widgets with no defect is approximately 0.0005 because this represents one event out of 20.

Triangular Distribution

The triangular distribution is a continuous probability distribution commonly used to model uncertain variables with a known minimum, maximum, and mode. It is characterized by three parameters – a, b, and c – which represent the minimum, maximum, and mode of the distribution, respectively.

For example, a construction company may use the triangular distribution to model the cost of a construction project. The minimum cost of the project may be $100,000, the maximum cost may be $500,000, and the most likely cost may be $300,000. The triangular distribution can be used to model the uncertainty in the project's cost and estimate the potential impact of cost overruns on the company's finances.

Another example of the triangular probability distribution is estimating the potential demand for a product or service. For instance, a retailer may use the triangular distribution to model the number of customers visiting its store on a given day. The minimum number of customers may be 100, the maximum number may be 500, and the most likely number may be 300. Using the triangular distribution, the retailer can estimate the range of potential demand for its products and develop appropriate inventory management strategies to meet customer demand.

PERT Distribution

The PERT (Program Evaluation and Review Technique) distribution is a continuous probability distribution commonly used in project management to model the uncertainty in project duration. It is characterized by three parameters – a, b, and c – representing the project's minimum, maximum, and most likely duration, respectively.

For example, a software development company may use the PERT distribution to model the duration of a software development project. The minimum duration of the project may be 6 months, the maximum duration may be 12 months, and the most likely duration may be 8 months. The PERT distribution can be used to model the uncertainty in the project's duration and estimate the potential impact of delays on the company's schedule and budget.

The PERT and triangular distribution are used to estimate the potential outcome of a project based on a range of possible values. However, there is a key difference between the two distributions in how they handle the most likely value.

In the PERT distribution, the most likely value is given more weight than the triangular distribution. The PERT distribution assumes that the most likely value is the most probable outcome and therefore assigns it a higher weight in the distribution. This means the PERT distribution is more accurate when the most likely value is a better estimate of the true value.

The PERT distribution achieves this using a three-point estimate that includes the minimum, most likely, and maximum values. The formula for calculating the PERT distribution takes into account the most likely value by using a weighted average:

Expected value = (minimum + 4 x most likely + maximum) / 6

The triangular distribution, on the other hand, assumes that all values within the range are equally likely, including the most likely value. This means the triangular distribution assigns equal weight to each value within the range. The formula for calculating the triangular distribution is simpler and uses only the minimum, most likely, and maximum values:

Expected value = (minimum + most likely + maximum) / 3

This means that the triangular distribution is more appropriate when there is no clear indication that the most likely value is more probable than any other value within the range.

The PERT distribution and the triangular distribution are useful tools for estimating the potential outcome of a project. However, the PERT distribution is more appropriate when the most likely value is a better estimate of the true value, as it assigns more weight to this value in the

distribution. Conversely, the triangular distribution is more appropriate when all values within the range are equally likely, including the most likely value.

Bernoulli Distribution

The Bernoulli distribution is a discrete probability model that takes the form of:
where P(X) is the probability of success and $0 < p < 1$. The mean and variance of this distribution are both equal to p, which makes sense since we are assuming that every trial has an equal chance of success or failure.

It is commonly used to model binary events, such as success or failure, or in the context of risk management, the presence or absence of a risk.

For example, a company may use the Bernoulli distribution to model the likelihood of a successful cyber attack on its computer network. If the company has a vulnerability that a cyber attacker can exploit, the Bernoulli distribution can be used to model the probability of a successful attack. This information can be used to estimate the likelihood of a successful attack and to develop appropriate risk management strategies.

The Bernoulli distribution can be used to "gamify" the comparison of strength between your defenses and the hacker.

Imagine a game where the two players are the company vs. the hacker. One player is highly skilled and has a 70% chance of winning each round, while the other player is less skilled and has a 30% chance of winning each round. The game continues until one player wins a total of 10 rounds.

We can use the Bernoulli distribution to determine each round's outcome. We would assign a value of 1 to the player who wins the round and 0 to the player who loses the round. We can then use the Bernoulli distribution to calculate the probability of each player winning the game.

For example, if the highly skilled player wins 7 rounds and the less skilled player wins 3 rounds, the probability of the highly skilled player winning the game is:

P(highly skilled player wins) = (0.7^7) x (0.3^3) = 0.027

Conversely, the probability of the less skilled player winning the game is:

P(less skilled player wins) = (0.3^7) x (0.7^3) = 0.00018

This means that the highly skilled player is much more likely to win the game, with a probability of approximately 2.7%. In contrast, the less skilled player has a much lower probability of winning, with a probability of approximately 0.018%.

By using the Bernoulli distribution to determine the outcome of each round and the probability of each player winning the game, we can create a challenging and engaging game. Players can strategize and make decisions based on the probability of winning each round, and the game's outcome is uncertain and exciting.

Additionally, we can adjust the probability of each player winning to make the game more or less challenging, depending on the desired level of difficulty. For example, we could increase the probability of the less skilled player winning to make the game more fair or decrease the probability of the highly skilled player winning to make the game more challenging.

The Bernoulli distribution is useful for gamifying interactions between two unequally opposing actors. By assigning a probability of winning or losing to each player and using the Bernoulli distribution to calculate the outcome of each round and the probability of each player winning the game, we can create a game that is both challenging and engaging and can be adjusted to suit varying levels of skill.

Probability distributions are an essential tool for quantifying risk. They provide a mathematical framework for modeling the likelihood of risks and their potential impact on an organization. The Poisson distribution can be used to model the frequency of rare events, the triangular distribution can be used to model uncertain variables with known minimum, maximum, and mode, the PERT distribution can be used to model the uncertainty in project duration, and the Bernoulli distribution can be used to model binary events. By using these probability distributions, organizations can better understand their risks and develop appropriate risk management strategies to mitigate the impact of risks.

FAIR™

The FAIR™ (Factor Analysis of Information Risk) standard model is a quantitative risk assessment model used to assess and quantify cyber risk. The model is based on the principles of factor analysis, which is a statistical method used to identify and analyze the underlying factors that contribute to a particular outcome. The FAIR™ model is designed to provide a consistent and repeatable method for assessing cyber risk, and organizations worldwide use it.

The FAIR™ model consists of six steps, which are as follows:

1. Define the scope and context of the analysis
2. Identify the assets and their value

3. Identify the threats and their frequency
4. Identify the vulnerabilities and their likelihood
5. Determine the impact of the risk
6. Calculate the risk

Step 1: Define the scope and context of the analysis.
The first step in the FAIR™ model is to define the scope and context of the analysis. This involves identifying the systems, data, and processes that will be included in the analysis, as well as the business objectives that are being supported. The scope and context of the analysis will help to ensure that the analysis is focused on the most important areas of the organization and that the results are relevant and actionable.

Step 2: Identify the assets and their value.
The second step in the FAIR™ model is to identify the assets and their value. This involves identifying the information assets critical to the organization and assigning a value to each asset based on its importance to the business. The value of an asset is typically based on its availability, confidentiality, and integrity, and it is used to determine the potential impact of a cyber attack on the organization.

Step 3: Identify the threats and their frequency.
The third step in the FAIR™ model is identifying the threats and their frequency. This involves identifying the potential sources of cyber threats, such as hackers, malware, or insider threats, and determining the frequency with which these threats are likely to occur. The frequency of a threat is typically based on historical data, industry trends, and expert opinion, and it is used to determine the likelihood of a cyber attack occurring.

Step 4: Identify the vulnerabilities and their likelihood.
The fourth step in the FAIR™ model is to identify the vulnerabilities and their likelihood. This involves identifying the weaknesses in the organization's systems, processes, and controls and determining the likelihood that a cyber attacker will exploit these weaknesses. The likelihood of a vulnerability being exploited is typically based on historical data, industry trends, and expert opinion, and it is used to determine the likelihood of a cyber attack being successful.

Step 5: Determine the impact of the risk.
The fifth step in the FAIR™ model is to determine the impact of the risk. This involves assessing the potential consequences of a cyber attack on the organization, such as financial loss, reputational damage, or regulatory fines. The impact of a cyber attack is typically based on the value of the assets that are at risk, as well as the likelihood of the attack being successful.

Step 6: Calculate the risk.
The last step in the FAIR™ model is to calculate the risk. This involves combining the likelihood of a cyber attack occurring with the potential impact of the attack to determine the overall risk level. The risk level is typically expressed as a probability of loss, such as a percentage or a dollar amount, and it is used to prioritize risk mitigation efforts and allocate resources.

The FAIR™ model is based on the principles of factor analysis, which is a statistical method used to identify and analyze the underlying factors that contribute to a particular outcome. The model is designed to provide a consistent and repeatable method for assessing cyber risk, and it is widely used by organizations around the world.

The FAIR™ model is based on several key assumptions and principles, which are as follows:

- Risk is a function of the likelihood of an event occurring and the impact of that event.
- Risk can be quantified using a probabilistic approach.
- Risk can be broken down into its component parts, such as threats, vulnerabilities, and assets.
- Risk can be managed by reducing the likelihood of an event occurring, reducing the impact of an event, or transferring the risk to another party.

The FAIR™ model is designed to be flexible and adaptable to different types of organizations and industries. The model can be customized to reflect the unique risk profile of an organization, and it can be used to assess a wide range of cyber risks, such as data breaches, cyber attacks, and insider threats.

The FAIR™ standard model is a quantitative risk assessment model used to assess and quantify cyber risk. The model is based on the principles of factor analysis, which is a statistical method used to identify and analyze the underlying factors that contribute to a particular outcome. The FAIR™ model is designed to provide a consistent and repeatable method for assessing cyber risk, and organizations worldwide use it. The model consists of six steps to identify the assets, threats, vulnerabilities, and potential impact of a cyber attack and calculate the overall risk level. The FAIR™ model is a powerful tool for managing cyber risk, and it can be customized to reflect the unique risk profile of an organization.

Vulnerability Analysis

Vulnerability analysis is a critical component of any comprehensive cybersecurity strategy. It involves identifying and assessing vulnerabilities in an organization's systems and applications and determining the likelihood and potential impact of a successful cyber attack. One way to perform vulnerability analysis is by using a SCAP (Security Content Automation Protocol)

scanner to collect data on vulnerabilities. We will explore using SCAP scanner data for vulnerability analysis and discuss how keywords can be identified for analysis.

Using SCAP Scanner Data for Vulnerability Analysis

A SCAP scanner is a tool that can be used to collect data on vulnerabilities in an organization's systems and applications. SCAP scanners use a standardized set of protocols to collect data on vulnerabilities, and they can be used to scan a wide range of systems and applications, including operating systems, web applications, databases, and network devices.

SCAP scanner data can be used to identify and assess vulnerabilities in an organization's IT infrastructure. This data can be used to prioritize vulnerabilities based on their severity and potential impact, and it can be used to develop a plan for mitigating these vulnerabilities.

Identifying Keywords for Analysis

One way to analyze SCAP scanner data is by identifying keywords associated with vulnerabilities. Keywords can be used to identify patterns and trends in the data, and they can be used to prioritize vulnerabilities based on their severity and potential impact.

To identify keywords for analysis, it is important first to understand the types of vulnerabilities in the organization's IT infrastructure. This can be done by reviewing the results of the SCAP scanner data and identifying the most common types of vulnerabilities present.

Once the types of vulnerabilities have been identified, keywords can be selected based on the following criteria:

- **Severity**: Keywords should be selected based on the severity of the vulnerability. For example, keywords such as "critical," "high," and "medium" can be used to identify vulnerabilities that pose the greatest risk to the organization.
- **Type of Vulnerability**: Keywords should be selected based on the type of vulnerability. For example, keywords such as "SQL injection," "cross-site scripting," and "buffer overflow" can be used to identify vulnerabilities that are commonly associated with specific types of attacks.
- **Frequency**: Keywords should be selected based on the frequency of the vulnerability. For example, keywords such as "frequently exploited," "commonly targeted," and "widely known" can be used to identify vulnerabilities that are most likely to be exploited by cyber attackers.

Once keywords have been identified, they can be used to analyze the SCAP scanner data and prioritize vulnerabilities based on their severity and potential impact. This can help organizations to develop a plan for mitigating vulnerabilities and reducing the risk of cyber attacks.

Vulnerability analysis is an essential component of any comprehensive cybersecurity strategy. SCAP scanners can be used to collect data on vulnerabilities in an organization's systems and applications, and this data can be used to identify and assess vulnerabilities in the organization's IT infrastructure. By identifying keywords for analysis, organizations can prioritize vulnerabilities based on their severity and potential impact and develop a mitigation plan. By implementing effective vulnerability analysis techniques, organizations can reduce the risk of cyber attacks and protect their systems and data from unauthorized access, theft, and disruption.

Cross-tab Tables for Analysis

A cross-tab layout is a common tool used in data analysis to summarize and analyze large datasets. It visually represents the relationships between two or more variables in a dataset. It can help to identify patterns, trends, and correlations that may be difficult to see in raw data. We will explore the use of the cross-tab layout for data analysis.

The cross-tab layout consists of a table that displays the frequency distribution of two or more variables in a dataset. The table is organized into rows and columns, with each row representing a category of one variable and each column representing a category of another variable. The table's cells contain the frequency or count of the number of observations in each category.

One of the primary benefits of the cross-tab layout is that it allows analysts to identify patterns and trends in large datasets quickly. For example, suppose an analyst is interested in understanding the relationship between gender and income. In that case, they can create a cross-tab layout that shows the frequency distribution of these two variables. This can help to identify any gender-based income disparities that may exist in the dataset.

Another benefit of the cross-tab layout is that it can be used to identify correlations between variables. For example, suppose an analyst is interested in understanding the relationship between age and education level. In that case, they can create a cross-tab layout that shows the frequency distribution of these two variables. This can help to identify any correlations between age and education level, such as whether younger individuals are more likely to have higher levels of education.

The cross-tab layout can also be used to summarize data in a way that is easy to understand and interpret. For example, suppose an analyst is interested in understanding the distribution of a particular variable, such as income. In that case, they can create a cross-tab layout that shows the frequency distribution of income by age group. This can help to identify any age-related income disparities that may exist in the dataset.

One limitation of the cross-tab layout is that it can be difficult to analyze datasets with a large number of variables. For example, suppose an analyst is interested in analyzing a dataset with ten or more variables. In that case, creating a cross-tab layout that accurately summarizes the relationships between all variables may be difficult. In these cases, other data analysis techniques, such as regression analysis or factor analysis, may be more appropriate.

The cross-tab layout is a powerful tool for data analysis that can help analysts to identify patterns, trends, and correlations in large datasets. It is a simple and easy-to-understand way of summarizing data and can be used to identify relationships between two or more variables. While the cross-tab layout has some limitations when it comes to analyzing datasets with a large number of variables, it remains a valuable tool for data analysis in many different fields.

Compliance Risk

Quantification of compliance risk is a critical component of any comprehensive cybersecurity strategy. It involves identifying and assessing compliance risks associated with an organization's IT infrastructure and determining the potential impact of non-compliance with regulatory requirements. One way to quantify compliance risk is using the NIST (National Institute of Standards and Technology) framework. We will explore the use of the NIST framework for quantifying compliance risk.

The NIST framework is a comprehensive set of guidelines and best practices for managing cybersecurity risk. It is widely used by organizations in both the public and private sectors, and it provides a structured approach to managing cybersecurity risk. The NIST framework consists of five core functions: identify, protect, detect, respond, and recover.

The first step in quantifying compliance risk using the NIST framework is identifying the regulatory requirements that apply to the organization's IT infrastructure. This can include data privacy, protection, and information security requirements. Once the regulatory requirements have been identified, the organization can use the NIST framework to assess its compliance.

The identify function of the NIST framework can be used to identify the assets subject to regulatory requirements. This can include data, systems, applications, and networks. The identify function can also be used to identify the threats that may impact these assets and the vulnerabilities that cyber attackers may exploit.

The protect function of the NIST framework can be used to implement security controls to protect the assets subject to regulatory requirements. This can include access controls, encryption, and data backup and recovery procedures. The protect function can also be used to implement security awareness training programs to reduce the risk of human vulnerabilities.

The detect function of the NIST framework can be used to detect potential compliance violations. This can include monitoring network traffic, system logs, and user activity. The detect function can also be used to implement intrusion detection and prevention systems to identify and prevent cyber attacks.

The respond function of the NIST framework can be used to respond to compliance violations. This can include incident response procedures, forensic analysis, and remediation activities. The respond function can also be used to report compliance violations to regulatory authorities.

The recover function of the NIST framework can be used to recover from compliance violations. This can include data recovery procedures, system restoration, and business continuity planning.
By using the NIST framework to quantify compliance risk, organizations can comprehensively understand their compliance posture. This can help identify non-compliance areas, prioritize remediation activities, and reduce the risk of regulatory fines and penalties.

Quantifying compliance risk is essential for organizations subject to regulatory requirements related to data privacy, data protection, and information security. The NIST framework provides a structured approach to managing cybersecurity risk and can be used to assess an organization's compliance with regulatory requirements. By implementing effective compliance risk quantification techniques, organizations can reduce non-compliance risk and protect their systems and data from unauthorized access, theft, and disruption.

Industry Attacks

In today's digital age, cyber attacks have become a significant threat to businesses across all industries. Cybercriminals use a variety of tactics to gain unauthorized access to sensitive information, disrupt business operations, and steal valuable data. We will discuss the analysis of top industry attacks and the importance of using cross-tab tables to estimate vulnerability across all types of attacks.

Analyzing top industry attacks involves identifying the most common types of cyber attacks businesses in a particular industry are likely to face. This analysis can help businesses better understand the threats they face and develop strategies to mitigate them. Some of the most common types of cyber attacks include phishing attacks, malware attacks, ransomware attacks, and denial of service attacks.

Phishing attacks are one of the most common types of cyber attacks. They use fraudulent emails, text messages, or websites to trick individuals into providing sensitive information, such as login credentials or credit card numbers. Phishing attacks can be particularly effective

because they often appear to come from trusted sources, such as banks or other financial institutions.

Malware attacks involve malicious software to gain unauthorized access to a computer system or network. Malware can be delivered through various channels, including email attachments, infected websites, or infected software downloads. Once installed on a system, malware can steal sensitive information, disrupt business operations, or damage the system.

Ransomware attacks involve using malware to encrypt computer systems or network files. The attackers then demand payment in exchange for the decryption key needed to unlock the files. Ransomware attacks can be devastating because they can cause significant financial losses and disrupt business operations for extended periods.

Denial of service attacks involves using multiple computers to overwhelm a targeted system with traffic, making it unavailable to users. Denial of service attacks can be particularly effective against websites or other online services that rely on a steady stream of traffic to function properly.

Using cross-tab tables is an important tool for estimating vulnerability across all types of cyber attacks. Cross-tab tables allow businesses to examine the relationships between different variables, such as the types of cyber attacks they are likely to face and the vulnerabilities of their IT systems. By using cross-tab tables, businesses can identify the specific vulnerabilities in their IT systems that are most likely to be targeted by cybercriminals.

For example, a business might use a cross-tab table to examine the relationship between the types of cyber attacks they are likely to face and the vulnerabilities of their IT systems. They might find that their IT systems are particularly vulnerable to malware attacks and that these attacks are the most common type of cyber attack in their industry. Armed with this information, the business can take steps to improve the security of its IT systems, such as implementing stronger anti-malware software or improving employee training on how to recognize and avoid malware attacks.

Another benefit of using cross-tab tables is that they can help businesses to identify patterns and trends in their data that might not be immediately apparent. For example, a business might use a cross-tab table to examine the relationship between the frequency of cyber attacks and the size of its IT budget. They might find that cybercriminals are more likely to target businesses with smaller IT budgets. Armed with this information, the business can take steps to allocate more resources to IT security, such as hiring additional staff or investing in new security technologies.

Analyzing top industry attacks is important for businesses looking to improve their cybersecurity posture. Businesses can develop strategies to mitigate those threats and protect their sensitive information by identifying the most common types of cyber attacks in their industry. Using cross-tab tables is an important tool for estimating vulnerability across all types of cyber attacks. By examining the relationships between different variables, businesses can identify specific vulnerabilities in their IT systems and take steps to improve their cybersecurity posture.

Attack Scenario

In today's digital age, cyber risk has become a significant concern for businesses of all sizes and industries. Cyber attacks can cause significant financial losses, damage a company's reputation, and disrupt business operations. To effectively manage cyber risk, businesses must understand the potential threats they face and the likelihood of them occurring. We will discuss scenario analysis, threat calculation, and likelihood estimation to quantify cyber risk.

Scenario analysis involves the creation of hypothetical scenarios that describe potential cyber attacks and their potential impact on a business. These scenarios can be based on historical data, industry trends, or other factors that are relevant to a particular business. By creating these scenarios, businesses can better understand their potential risks and develop strategies to mitigate them.

Threat calculation involves the identification and assessment of potential cyber threats. This process involves examining the different types of cyber attacks a business may face, such as phishing attacks, malware attacks, or denial-of-service attacks. Once these threats have been identified, they are assessed based on their potential impact on the business, such as the financial losses that may result from a successful attack.

Likelihood estimation involves the assessment of the probability that a particular cyber threat will occur. This process involves examining the factors that may increase or decrease the likelihood of a successful attack, such as the strength of a business's cybersecurity defenses or the sophistication of the attackers. By estimating the likelihood of different cyber threats, businesses can prioritize risk management efforts and allocate resources more effectively.

To quantify cyber risk, businesses can use a combination of scenario analysis, threat calculation, and likelihood estimation. By combining these approaches, businesses can develop a comprehensive understanding of the potential risks they face and the likelihood of those risks occurring.

For example, a business might use scenario analysis to create a hypothetical scenario in which their customer data is stolen in a cyber attack. They might then use threat calculation to assess

the potential impact of such an attack, such as the financial losses resulting from losing customer trust. Finally, they might use likelihood estimation to assess the probability of such an attack occurring based on factors such as the strength of their cybersecurity defenses and the likelihood of a successful phishing attack.

By combining these approaches, businesses can develop a quantitative estimate of their cyber risk. This estimate can be used to inform risk management decisions, such as the allocation of resources to improve cybersecurity defenses or the purchase of cyber insurance to mitigate financial losses.

One of the benefits of using scenario analysis, threat calculation, and likelihood estimation to quantify cyber risk is that it allows businesses to prioritize their risk management efforts. By identifying the most significant threats and estimating the likelihood of them occurring, businesses can focus their resources on the areas of greatest risk. This can help to ensure that risk management efforts are effective and efficient.

Another benefit of these approaches is that they allow businesses to understand their cyber risk better. By examining the potential impact of different types of cyber attacks and estimating the likelihood of those attacks occurring, businesses can develop a more nuanced understanding of the risks they face. This can help ensure that risk management efforts are tailored to the business's specific needs.

Using scenario analysis, threat calculation, and likelihood estimation is an effective way to quantify cyber risk. By combining these approaches, businesses can develop a quantitative estimate of their cyber risk and prioritize their risk management efforts accordingly. This can help businesses be prepared to manage cyber risk effectively and protect their sensitive information from potential threats.