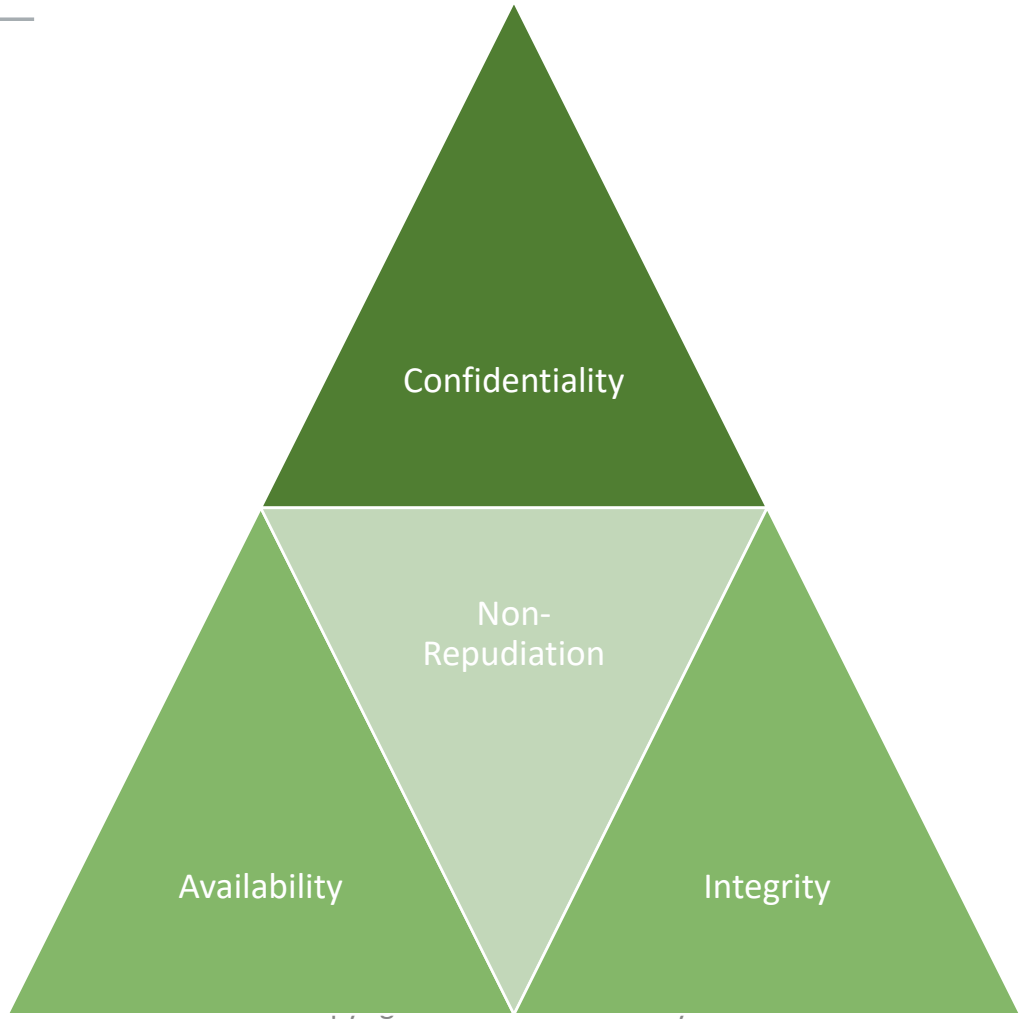
System Security Group | Lancaster University

Introduction to Cybersecurity Risk Management

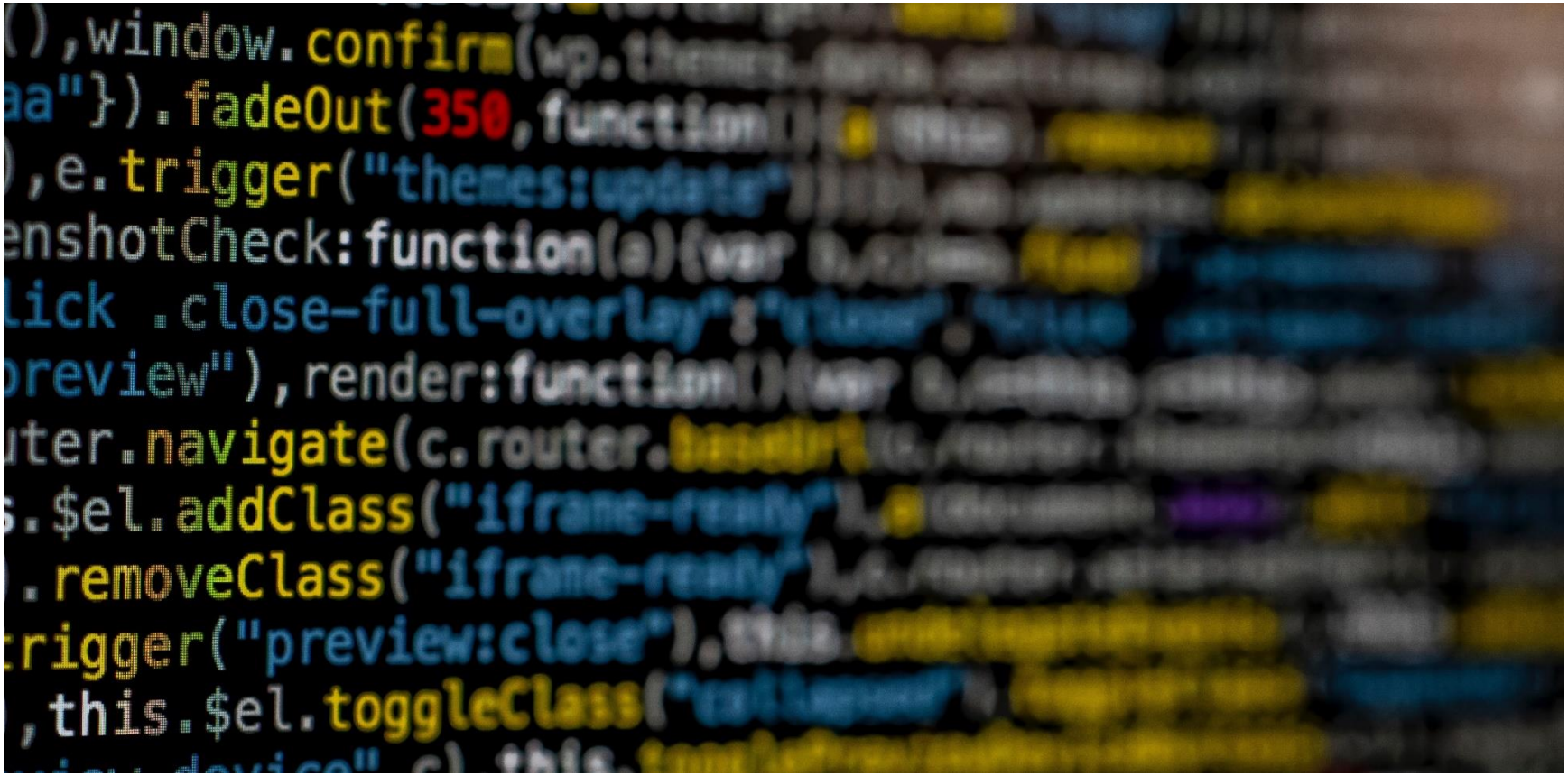
Aims

- Understand the fundamental topics and key terms
- Understand the importance of risk management in defence and protection of systems

Confidentiality, Integrity and Availability with Non-Repudiation



What is a Cyber Attack?



Threat Agents, Threats and Attacks

- Threat Agents gives rise to a Threats
  - Threats are the possibility of damaging actions
    - Threats are made against socio-technical systems

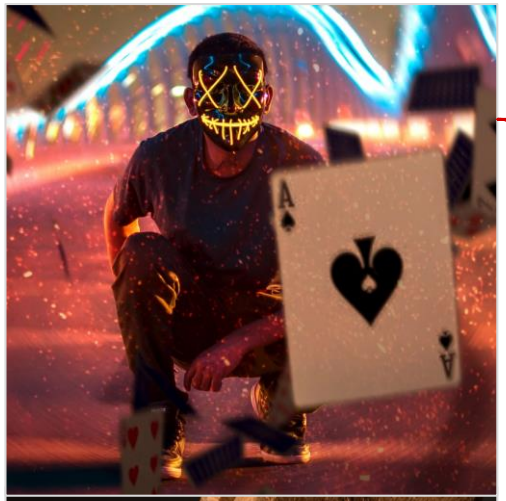
Vulnerabilities, Exploits, Payloads and Actions

System Security Group | Lancaster University

- Vulnerabilities are used by Exploits
  - Exploits carry a Payload
    - Payloads achieves the intended objective

What is Risk?

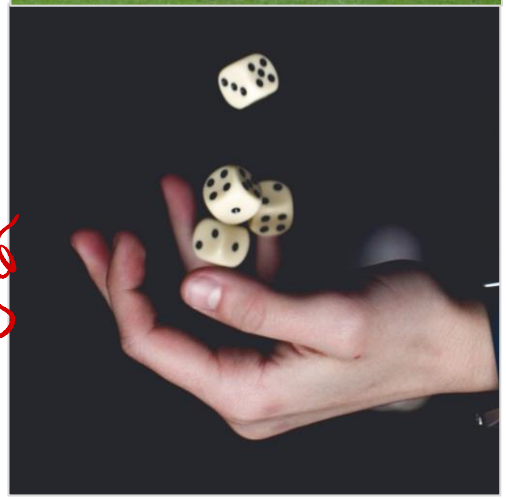
Sources of Uncertainty



Who is the Attacker?

What is there Goal?

How likely is it they will succeed?

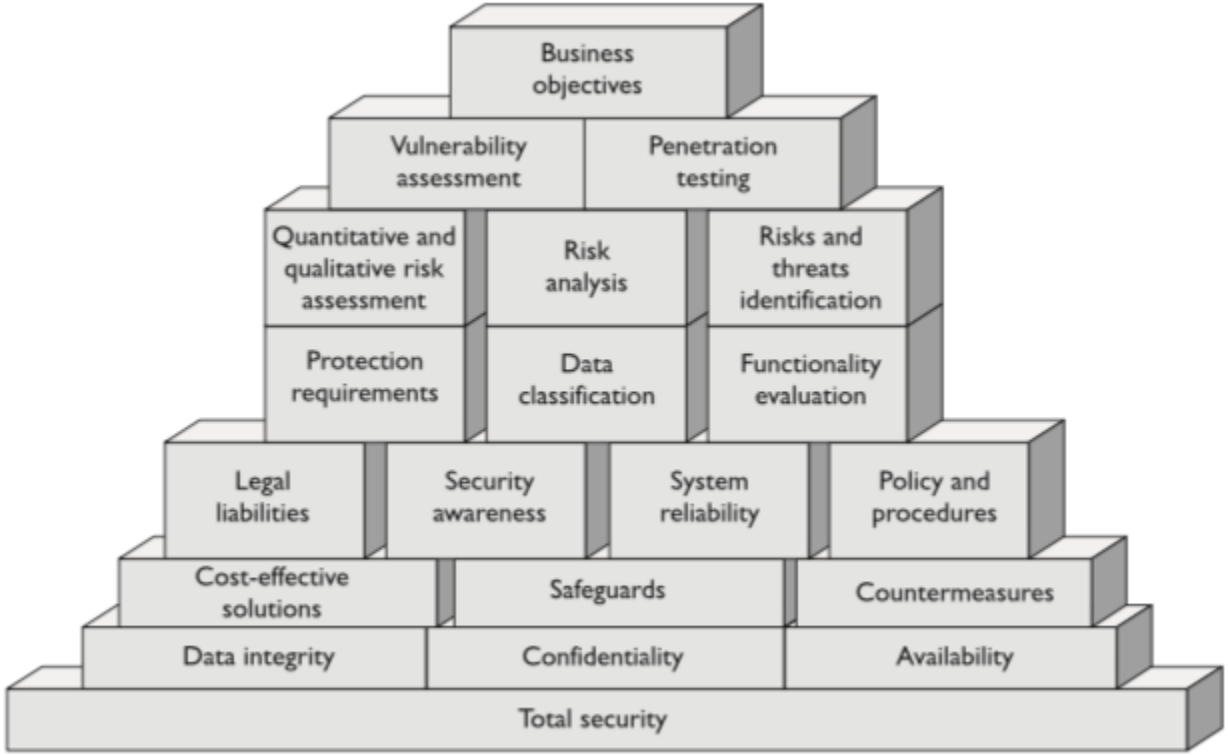


What is the impact if they do?

Risk Management and Risk Assessment

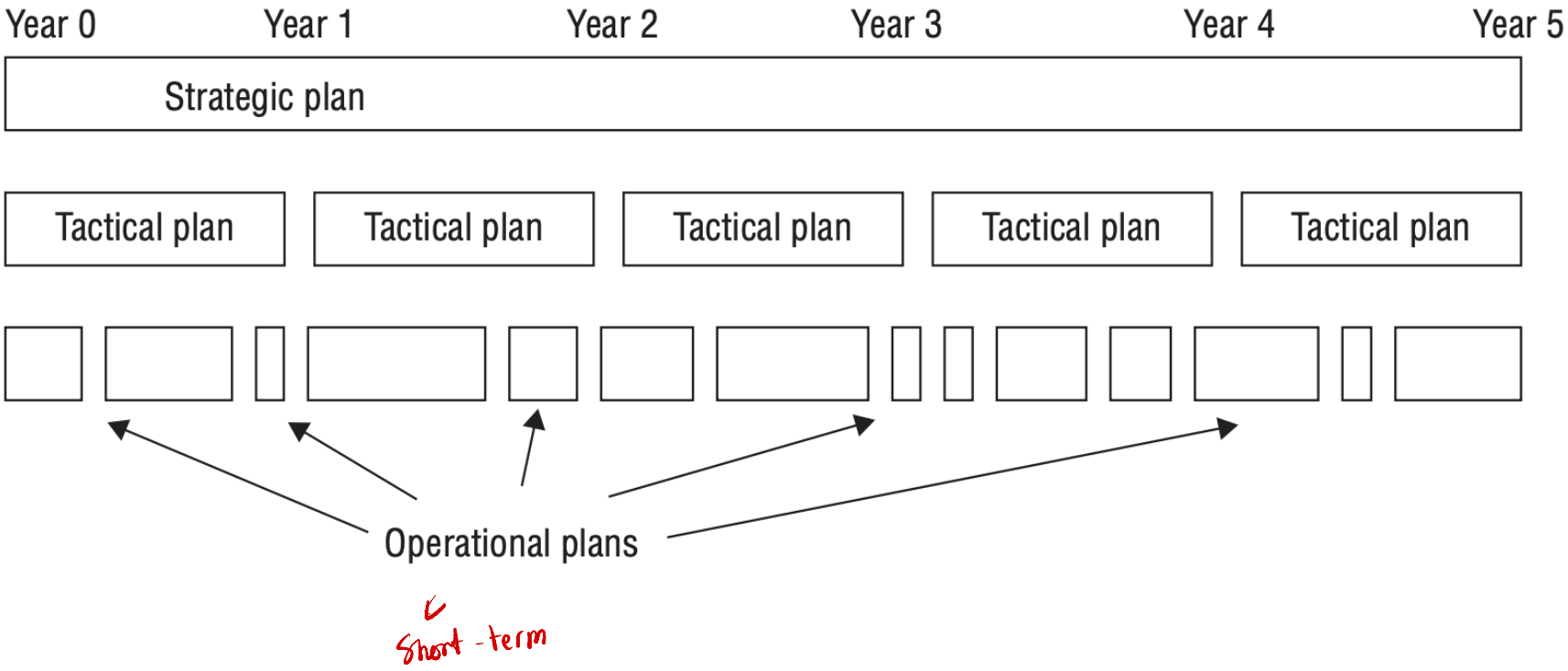
- Risk Management is organisational control to risk
  - Risk Assessment is Identification, Analysis and Evaluation
    - Risk Analysis enables comprehension of risk

Total Security Building Blocks



Strategy, Tactic and Operation

System Security Group | Lancaster University



Qualitative Assessment

- Scenarios of risk possibilities,
- Rank the seriousness of the threats,
- Validity of countermeasures.
- Relies in judgement, best practices, intuition, experience.
- Techniques:
  - Delphi,
  - Brainstorming,
  - Storyboarding,
  - Focus groups,
  - Surveys

Quantitative Risk Assessment/Analysis

- Attempt to assign meaningful numbers against e.g.: Safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, etc…
- Attempt to assign meaningful percentages against probability of likelihood.

CISSP Example Risk Analysis Steps

System Security Group | Lancaster University

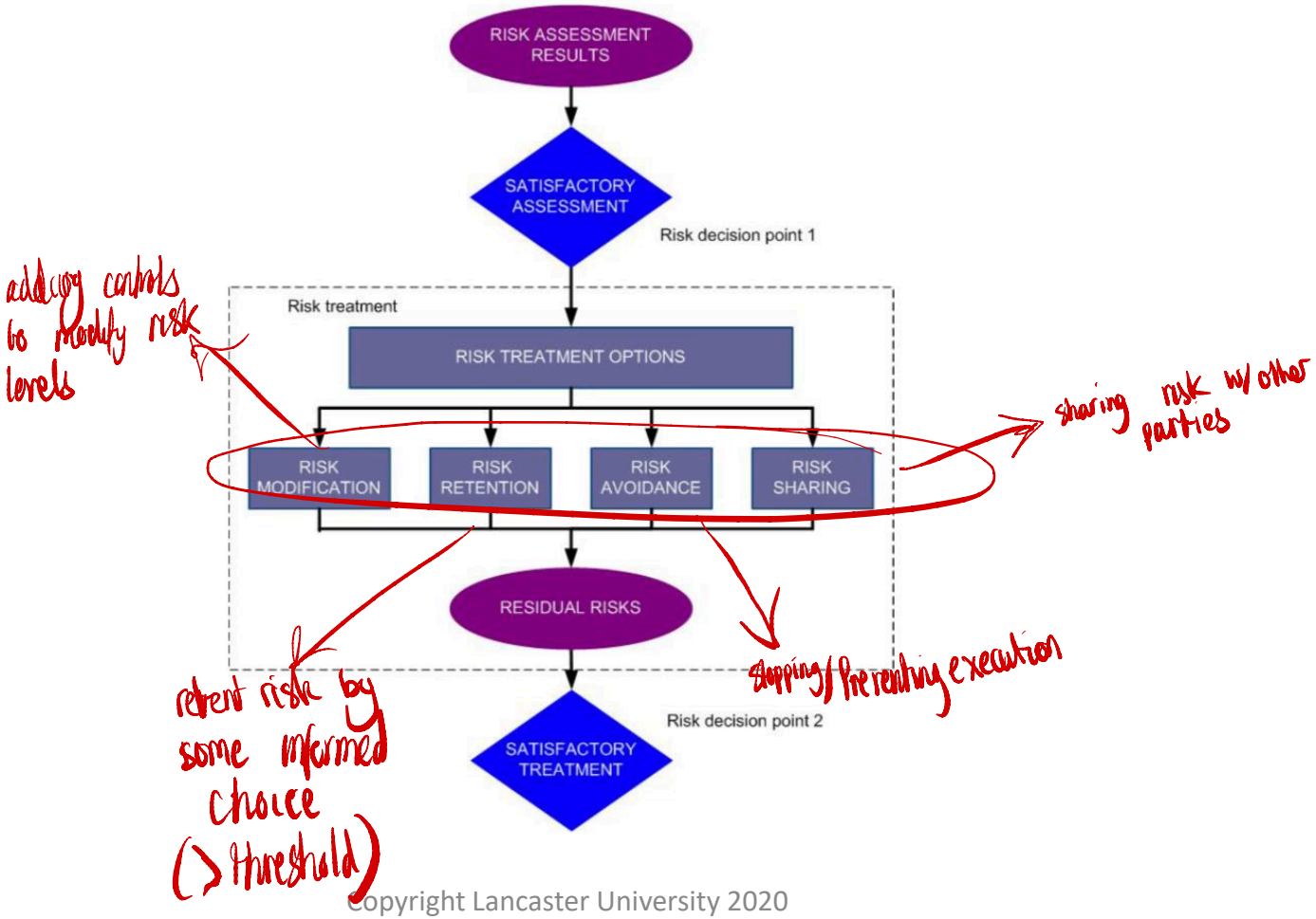
1. Identify assets and their value
2. Estimate potential loss per threat
3. Perform Threat analysis, calculate ARO
4. Derive the ALE per threat
5. Reduce, Transfer, Avoid or Accept the Risk

Exposure and Loss Expectancy

The estimated monetary loss expected from a given threat over a year

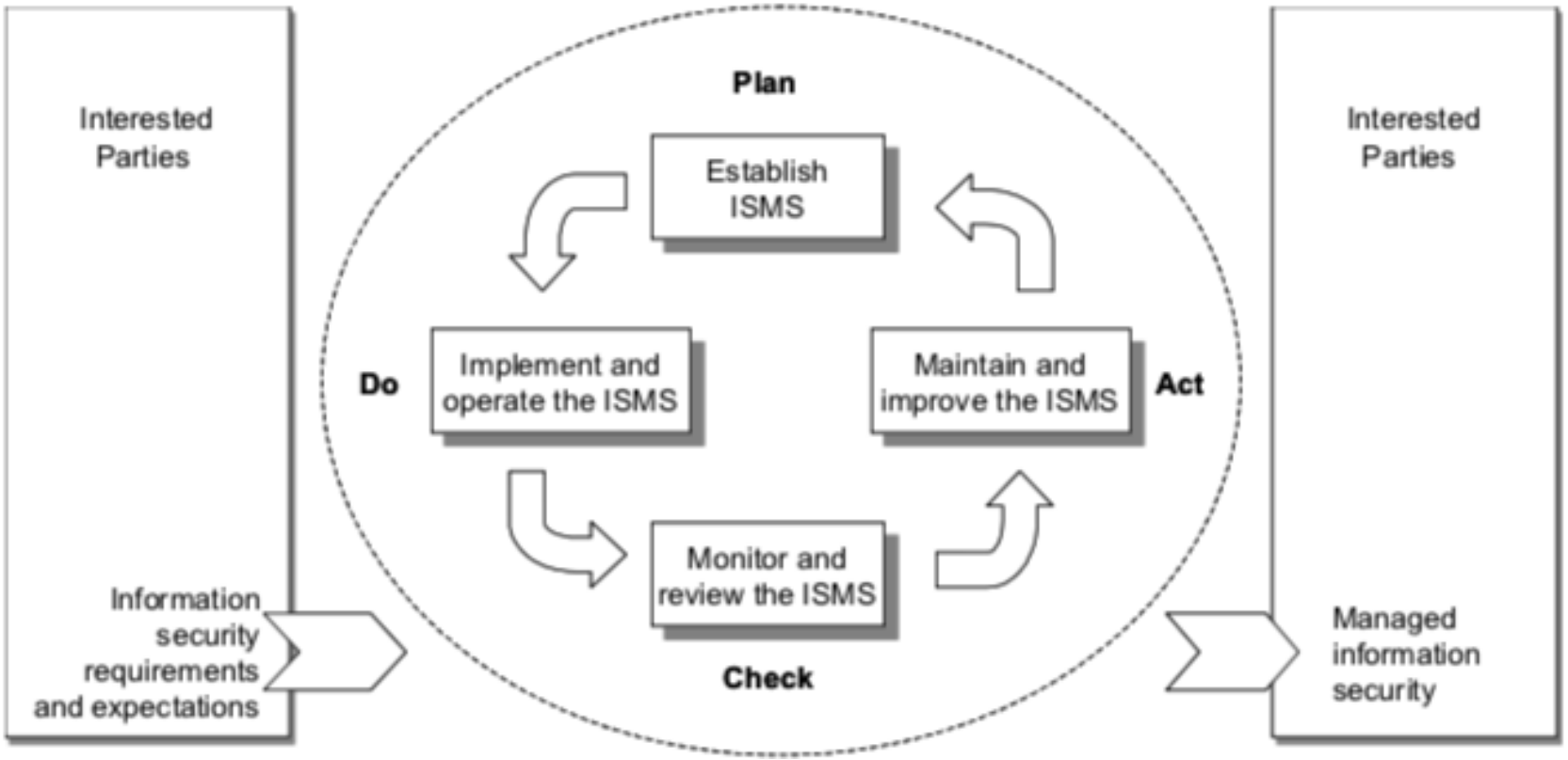
- Annual Rate of Occurrence x Single Loss Expectance
  - 10% x £550,000 = £55,000

Risk Treatment



Security Controls

Plan Do Check Act



Residual Risk

Incident Management

ability to detect, monitor, deal w/, report, and learn from security incidents

Questions?

System Security Group | Lancaster University

References

- Harris, S. (2010). CISSP All-in-One Exam Guide (5th ed.). New York: McGraw-Hill.
- https://mrcissp.com/2019/01/09/cia-triad-in-details-looks-simple-but-actually-complex/
- Chapple, M., Stewart, J.M. and Gibson, D., 2018. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. New York: John Wiley & Sons
- British Standards Institute. (2005). BS ISO/IEC 27001 - Information Technology - Security Techniques – Information Security Management Systems - Requirements. Retrieved from https://bsol.bsigroup.com/Search/Search?searchKey=27001
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
- British Standards Institute. (2011). BS ISO/IEC 27005 - Information Technology - Security Techniques – Information Security Risk Management. Retrieved from https://bsol.bsigroup.com/Search/Search?searchKey=27005
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- https://www.ncsc.gov.uk/collection/risk-management-collection?curPage=/collection/risk-management-collection/essential-topics/fundamentals

System Security Group | Lancaster University

Fundamentals of Statistics

Describing the Centre

- The central tendency
- Where is the middle of the data
- Arithmetic Mean
- Median
- Mode

An Arithmetic Mean Example

- Our population is composted of 11 computers and we are measuring the number of applications installed on each
  - 1,2,6,2,1,1,4,7,3,20,8
  - The arithmetic mean is the sum of the data points divided by the number of data points
  - $\frac{1+2+6+2+1+1+4+7+3+20+8}{11} = \frac{55}{11} = 5$

A Median Example

- Using our example from before we have the following numbers of applications installed
  - 1,2,6,2,1,1,4,7,3,20,8
- The median is found by ordering the population and then taking the mid point.
  - 1,1,1,2,2,3,4,6,7,8,20
  - The median is therefore 3
  - If we had only 10 samples we would take the arithmetic mean of the two middle numbers

A Mode Example

- The mode is the most common number.
- In our sample of
  - 1,2,6,2,1,1,4,7,3,20,8
- In this case the most frequent number is 1
  - The mode is 1

Measuring the Spread

- How close are all the data points around out measure of central tendency?
- Median → Interquartile range
- Mean → Variance or standard deviation

Interquartile range

- We want to know the range from
  - the mid way point between the first number and the median
  - The mid way point between the median and the last number
- 1,1,1,2,2,3,4,6,7,8,20
- 1,1,1,2,2,3,4,6,7,8,20
- IQR is 1 to 7 = 6

The Variance

- The average of the square distances of the population data points from the population mean
  - 1,2,6,2,1,1,4,7,3,20,8, mean of 5

$$\frac{(1-5)^2+(2-5)^2+(6-5)^2+(2-5)^2+(1-5)^2+(1-5)^2+(4-5)^2+(7-5)^2+(3-5)^2+(20-5)^2+(8-5)^2}{11}$$

  - The variance is approx. 28.08 = σ^2
  - The standard deviation is the $\sqrt{Variation} = \sigma$

$$\frac{\sum_{i=1}^{N}(x_i-\mu)^2}{N}$$

System Security Group | Lancaster University

Questions?

Fundamentals of Probability

Sets

- A **set** is a collection of objects called **elements** or **members**
  - Sets normally capital letters
  - Elements of a set normally lower case
- Membership is denoted by:
  - $a \in S$ a is a member of Set S (S normally means the complete sample space
  - $a \notin S$ a is not a member of Set S

Set Membership

- Memberships can be defined as a grouping or by properties
- Grouping S={a,b,c,d,e}
- Property S={x:$x\ has\ property\ P$} ← characteristic / prerequisite
  - S={N:$N \in Z$, $N \leq 500$}
  - where Z =$Set\ of\ all\ integer\ Numbers$
- If every element in set A is in set B and every element in set B is in set A then A=B
  - Otherwise $A \neq B$

Sub or Super?

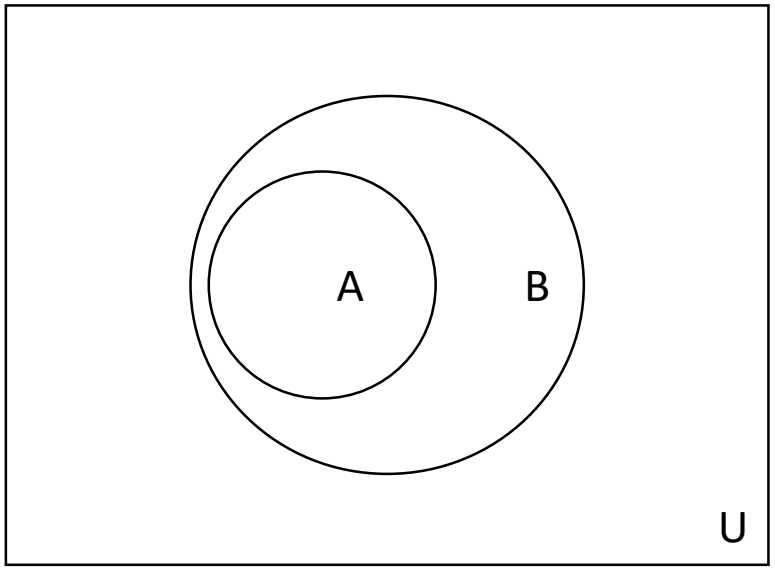
- If every element of A is an element of B then A is a subset of B, $A \subseteq B$
  - Also B is a superset of A, $B \supseteq A$
- If every element of A is an element of B but sets A and B are not equal then A is a proper subset of B, $A \subset B$
  - Also B is a proper superset of A, $B \supset A$
- Not a sub or super set then use:
  - $\not\subset$, $\not\supset$, $\not\subseteq$, $\not\supseteq$

Complements and Empties

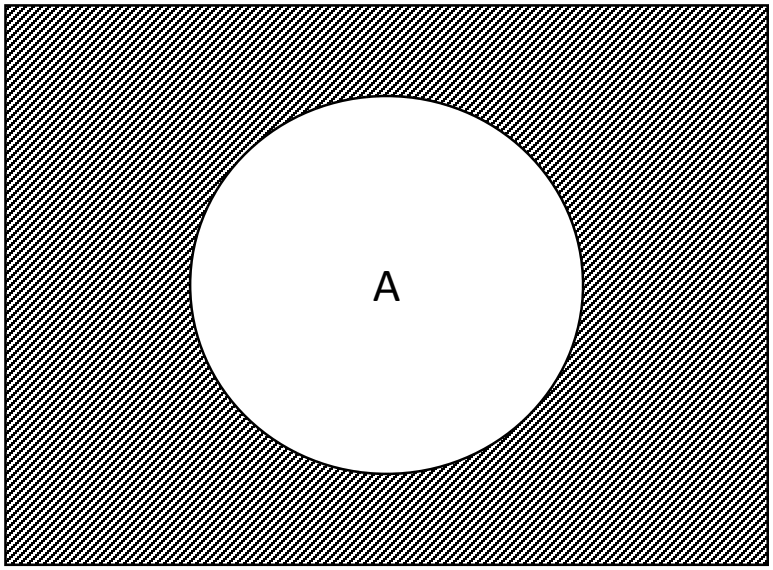
- An empty set is denoted by:
  - $A = \emptyset$
- The complement of a set A is everything that is not in A but still in the universal set U
  - $\bar{A} = \{x : x \in U, x \notin A\}$

Venn Diagrams

- These are really useful to understanding the relationships between sets:



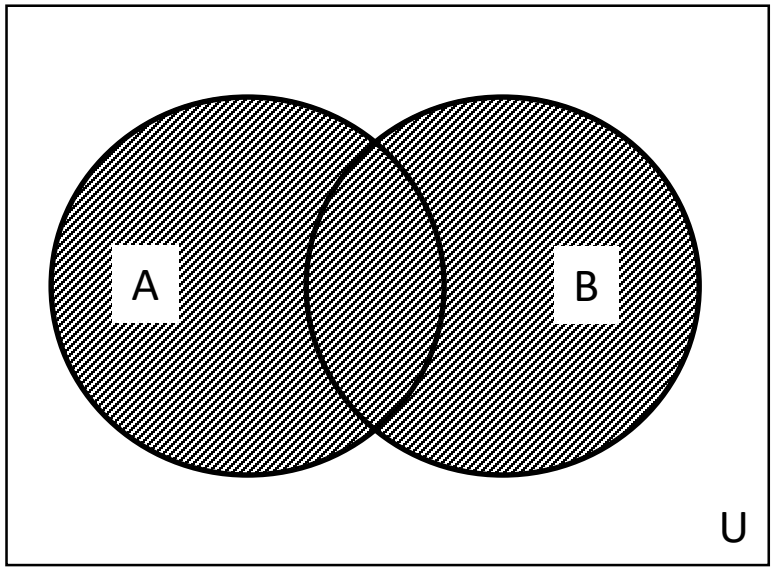
$A \subset B$



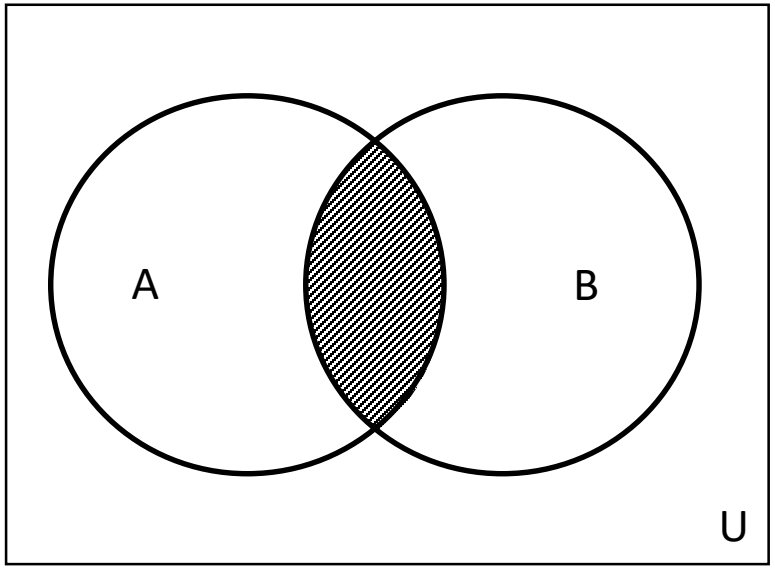
$\bar{A}\ (shaded)$

Union and Intersection

- Sets can be combined in two different ways **if they relate to the same universal set U**
  - Union: A or B
  - Intersection: A and B

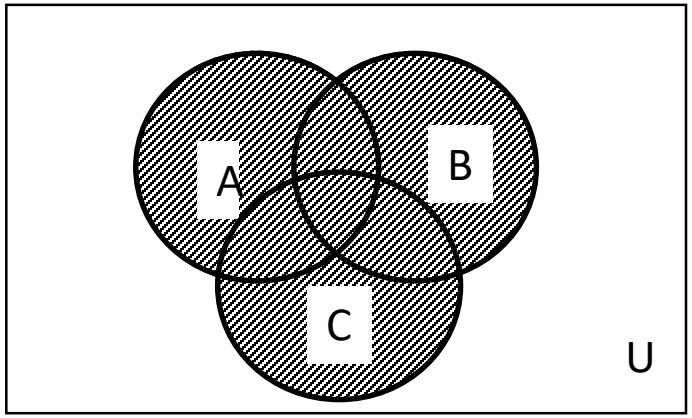


$A \cup B = B \cup A$

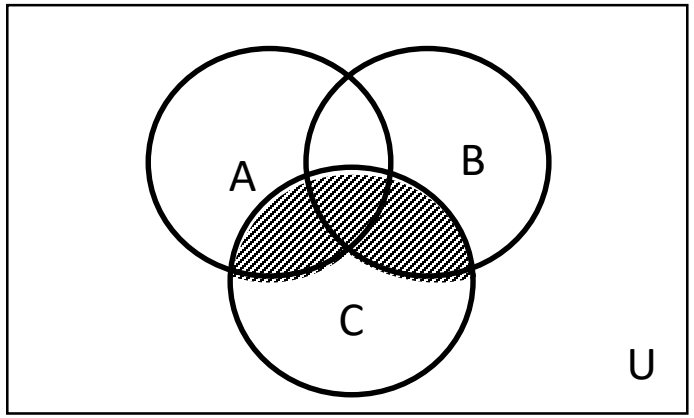


$A \cap B = B \cap A$

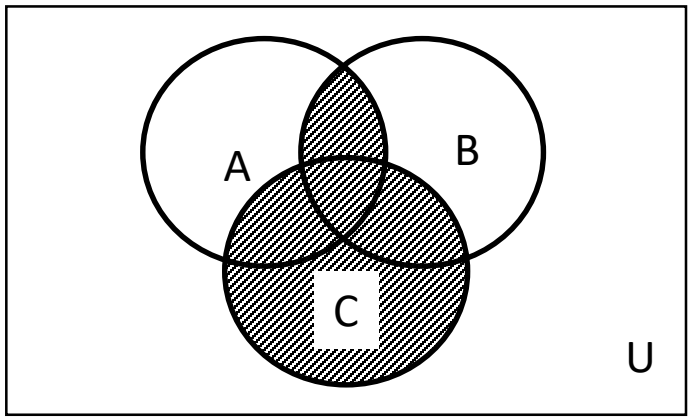
Algebra of Sets



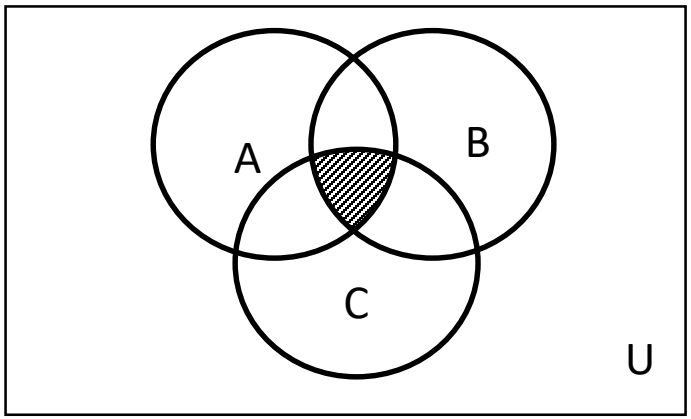
$C \cup (A \cup B)$



$C \cap (A \cup B)$



$C \cup (A \cap B)$



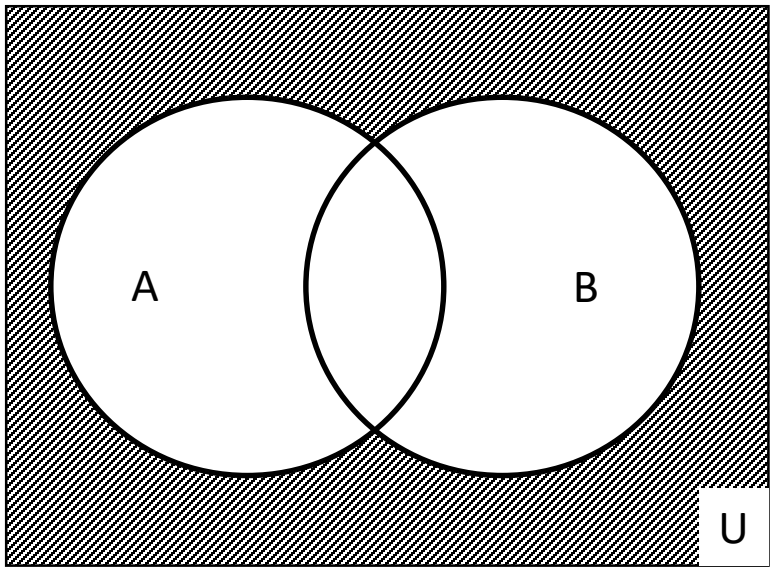
$C \cap (A \cap B)$

Algebra of Sets

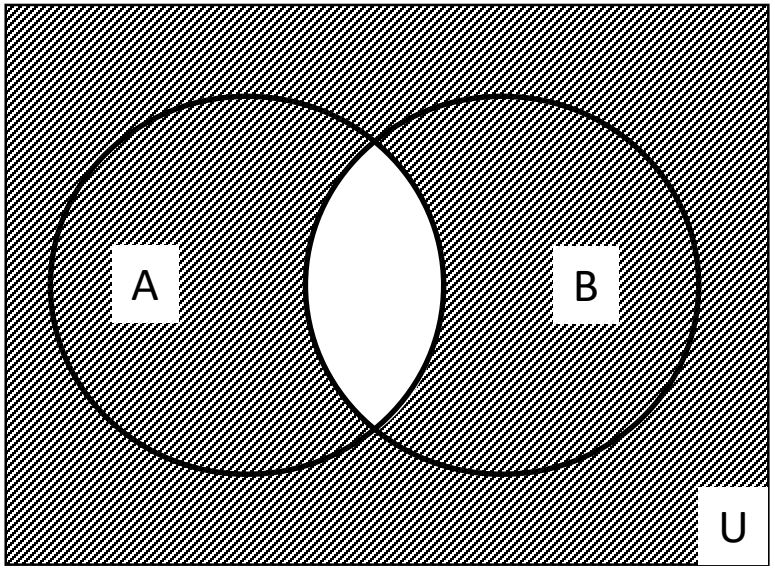
- Commutative Laws
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Identity Laws
  - $A \cup \phi = A$
  - $A \cap U = A$
- Associative Laws
  - $A \cup (\mathrm{B} \cup C) = (A \cup B) \cup C$
  - $A \cap (\mathrm{B} \cap C) = (A \cap B) \cap C$
- Idempotent Laws
  - $A \cup A = A$
  - $A \cap A = A$
- Complementary Laws
  - $A \cup \bar{A} = U$
  - $A \cap \bar{A} = \emptyset$
- Distributive Laws
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan Laws

- We can use the ∩,∪, (¯) operators to simplify expressions. These are called De Morgan laws.



$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$



$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

What Are Events?

Sample Space S={}

- The sample space defines everything that can happen:
- Discrete:
  - Written as a list $S = \{a, b, c\}$
- Continuous:
  - Measurement of a continuous variable i.e. height
  - Written as $S = (0,10)$ for open interval $0 < x < 10$
  - Written as $S = [0,10]$ for closed interval $0 \leq x \leq 10$

Events

- Events are what we observe and are subsets of S.
- The event is said to occur if an element of the event is measured.
- As events are sets then set operations apply to them
  - $A \cup B$: A or B occurs
  - $A \cap B$: A and B occur
  - $S - A$ or $\bar{A}$: not A occurs
  - $A = \emptyset$: The impossible event
  - $A = S$: The certain event

Axioms of Probability

Proper Subset

- $P(A)$ is the probability of the event $A \subseteq S$
- This assigns a probability to an event
- Axioms
  1. The certain event S has probability = 1: $P(S) = 1$
  2. All probabilities are positive: $P(A) \geq 0$
  3. Additional rule: if A and B are disjointed such that $A \cap B = \emptyset$ then: $P(A \cup B) = P(A) + P(B)$

Axioms of Probability

4. Complement rule: $P(S - A) = 1 - P(A)$
5. $P(\emptyset) = 0$
6. If $A \subseteq B$ then $P(A) \leq P(B)$
7. General Addition Rule:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Consider this through a Venn diagram. The overlap cannot count twice.

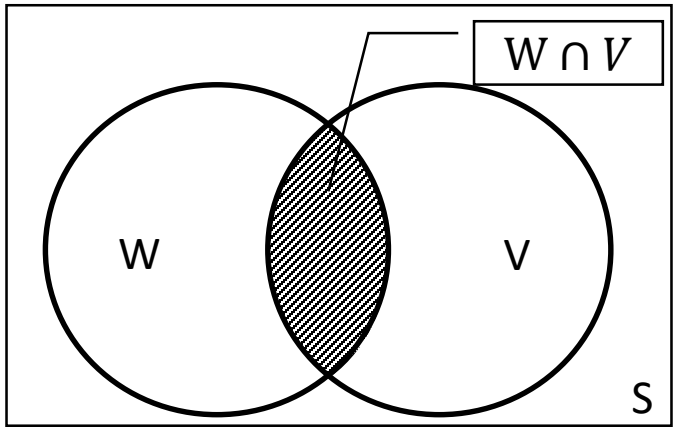
Example Problem

- During an analysis of machines on a network it is found that 80% of them were infected with a worm, 50% infected with a virus and that 40% infected with both. Find the probabilities of:
  1. A machine has either a worm OR a virus
  2. A machine has a worm but NOT a virus
  3. A machine is not infected.

Example Solution 1

Let W and V denote worm and virus infection respectively.

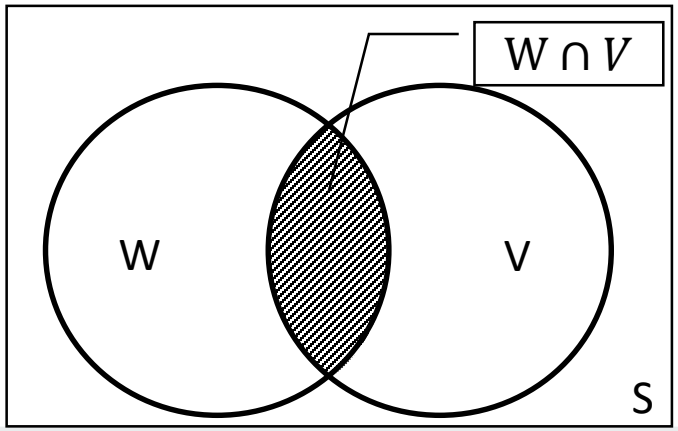
1. This is relatively easy as we can use the General addition rule. Therefore,
$$P(W \cup V) = P(W) + P(V) - P(W \cap V)$$
$$= 0.8 + 0.5 - 0.4 = 0.9$$



Example Solution 2

2. The group of machines with a worm includes those that have both and those with just a worm. Therefore, to find event where there are just those with a worm and no virus we need to know: $E = \{x : x \in (W \cap \bar{V})\}$

$$P(W \cap \bar{V}) = \mathrm{P}(\mathrm{W}) - \mathrm{P}(\mathrm{W} \cap V) = 0.8 - 0.4 = 0.4$$



Example Solution 3

3. Use De Morgan's Law and the answer from 1.

$$P(\bar{W} \cap \bar{V}) = P(\overline{W \cup V})$$

$$P(\overline{W \cup V}) = 1 - P(W \cup V)$$

$$= 1 - \big(P(W) + P(V) - P(W \cap V)\big)$$

$$= 1 - 0.8 - 0.5 + 0.4 = 0.1$$

System Security Group | Lancaster University

Questions?

Conditional Probabilities

Conditional Probability

- This allows us to deal with a probability if we know an event has already occurred
- What is the probability of event A GIVEN that event B has already occurred. $P(A|B)$
- We effectively have to scale the sample space to B, therefore:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Where $B \neq \emptyset \ \therefore P(B) > 0$

Conditional Probability Flipping

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \quad \text{Therefore } P(A|B)P(B) = P(A \cap B)$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} \quad \text{Therefore } P(B|A)P(A) = P(A \cap B)$$

Therefore

$$P(B|A)P(A) = P(A|B)P(B) = P(A \cap B)$$

Simple Example

- Probability that a fair dice role is even given that the result is less than 4.

$$R = \{1,2,3,4,5,6\}, P(R) = \frac{1}{6}$$

$$P(Even| < 4) = \frac{P(even \ \& < 4)}{P(< 4)}$$

$$E_{even\&<4} = \{x: x \in R, x < 4, x \ is \ even\} = \{2\}$$

$$E_{<4} = \{x: x \in R, x < 4\} = \{1,2,3\}$$

$$= \frac{P(\{2\})}{P(1,2,3\})} = \frac{\frac{1}{6}}{3 \times \frac{1}{6}} = \frac{1}{3}$$

Another Example

The probability of a machine being on the Internet is $P(I) = 0.92$. The probability it has a virus is $P(V) = 0.82$. The probability it has a virus and is on the Internet is $P(V \cap I) = 0.78$

1. Probability it has a virus given it is on the Internet, $P(V|I)$
2. Probability it does not have a virus given it is not on the Internet, $P(\bar{V}|\bar{I})$

Another Example Solution 1

1. Simple conditional probability:

$$P(V|I) = \frac{P(V \cap I)}{P(I)}$$

$$= \frac{0.78}{0.92} = 0.85$$

Another Example Solution 2

2. A bit more complicated!

$$P(\bar{V}|\bar{I}) = \frac{P(\bar{V} \cap \bar{I})}{P(\bar{I})}$$

$$P(\bar{V} \cap \bar{I}) = P(\overline{V \cup I})$$

$$P(\overline{V \cup I}) = 1 - \mathrm{P}(\mathrm{V} \cup I)$$

$$P(V \cup I) = P(V) + P(I) - P(V \cap I)$$

$$\therefore \; P(\bar{V}|\bar{I}) = \frac{1 - P(V) - P(I) + P(V \cap I)}{1 - P(I)}$$

$$= \frac{1 - 0.83 - 0.92 + 0.78}{1 - 0.92} = \frac{0.03}{0.08} = 0.38$$

Independence

- The probability of event B may be raised, lowered or stay the same, given A has occurred.
- If it stays the same they are independent
  - $P(B|A) = P(B)$
  - $P(A|B) = P(A)$
- Independence is symmetric between two events

Bayes and Bayesian Theory

- Bayes' theorem gives the relationship between P(A) and P(B), and P(A|B) and P(B|A).
- Enables us to update a probability given an observation.
  - The *prior probability*, is what we have before
  - The *posterior probability*, is what we get afterwards

Bayesian Example

- Example: 10% of all hosts have a security flaw. A screening procedure positively identifies security flaws 80% of the time and 10% of unflawed machines are incorrectly identified.
- Identify the probability that a machine has a flaw given the machine has tested positive for a flaw.

Bayesian Example Solution

- Consider the probabilities as frequencies:
  - Consider a sample space of 1000 machines
  - $P(F) = 0.1$ have flaws, therefore 100 machines
  - $P(\bar{F}) = 0.9$ are unflawed, therefore 900 machines
  - $P(+T|F) = 0.8$, 80 out of 100 flawed machines test positive.
  - $P(+T|\bar{F}) = 0.1$, 90 out of 900 unflawed machines test positive.
  - 170 Positive tests
  - Therefore $P(F|T) = \frac{80}{170} = 47\%$

90 + 80

Bayes Theorem

- The general theorem is:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

- Applying the law of total probability:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|\bar{A})P(\bar{A})}$$

Suggest you read: http://arbital.com/p/bayes_rule_guide

Bayes Theorem Example

Suppose that two factories supply light bulbs to the market. Factory X's bulbs work for over 5000 hours in 99% of cases, whereas factory Y's bulbs work for over 5000 hours in 95% of cases. It is known that factory X supplies 60% of the total bulbs available and Y supplies 40% of the total bulbs available. What is the chance that a purchased bulb will work for longer than 5000 hours?

Applying the law of total probability, we have:

$$P(A) = P(A \mid B_X) \cdot P(B_X) + P(A \mid B_Y) \cdot P(B_Y)$$

Different factors

$$= \frac{99}{100} \cdot \frac{6}{10} + \frac{95}{100} \cdot \frac{4}{10} = \frac{594 + 380}{1000} = \frac{974}{1000}$$

where

- $P(B_X) = \frac{6}{10}$ is the probability that the purchased bulb was manufactured by factory X;
- $P(B_Y) = \frac{4}{10}$ is the probability that the purchased bulb was manufactured by factory Y;
- $P(A \mid B_X) = \frac{99}{100}$ is the probability that a bulb manufactured by X will work for over 5000 hours;
- $P(A \mid B_Y) = \frac{95}{100}$ is the probability that a bulb manufactured by Y will work for over 5000 hours.

Thus each purchased light bulb has a 97.4% chance to work for more than 5000 hours.

Questions?