CSE 5338 HW 1.

Seung Ki Lee

35460312

Q1

Identification: This asks the question "Who are you?" Facebook identifies the user for NYT by the user's information such as ID and email address.

Authentication: This asks the question "Are you who you say you are?" Facebook Authenticates the user by requesting the login information.

Authorization: This asks the question "Do you have permission to do what you say you want to do?" the user authorizes NYT to access their information by clicking yes, and NYT authorizes users to use functions available to only logged in users.

Q2

a. FERPA form, that every student has to fill out every year is a classic example where confidentiality and availability clashes. It would be easier for both parents and students if you can just give out your academic record on demand, but that will increase the chance of unauthorized person getting hold of your sensitive personal information. Medical records are another example that possesses the same conflict.

b. Wikipedia is a good example where these two collide. For the availability of information Wikipedia relies on independent user submissions, but because of that very reason they cannot screen and guarantee that the information on the wiki has any integrity.

Q3

a.

Curve #3 is the most preferred. Both false positive and false negative are undesirable, and IC3 has the lowest value for both or them. The optimal point of utilities are all on IC3 as well. A general Utility function is:

$U(\alpha, \beta) = u \times \alpha + v \times \beta$

In this case, lower the value of α and β the higher the utility. So the accurate version of the function is:

$U(\alpha, \beta) = u \times \frac{1}{\alpha} + v \times \frac{1}{\beta}$

$Assume: u \sim v$

$(\alpha_3, \beta_3) < (\alpha_2, \beta_2) < (\alpha_1, \beta_1)$

$U(\alpha_3, \beta_3) > U(\alpha_2, \beta_2) > U(\alpha_1, \beta_1)$

$(\alpha_3, \beta_3) \in IC3$

Thus IC3 is most preferred.

b.

Given assumption is:

$(h, l) \sim (l, h)$

$(l, l) \succ (h, h)$

$(\alpha_h, \beta_l) \sim (\alpha_l, \beta_h)$

$(\alpha_l, \beta_l) \succ (\alpha_h, \beta_h)$

$U(\alpha, \beta) = u \times \alpha + v \times \beta$

For ease of calculation I will assign:

$\alpha_h = -1$

$\alpha_l = 1$

$\beta_h = -1$

$\beta_l = 1$

Combination	Total Utility
(α_h, β_h)	-2
(α_h, β_l)	0
(α_l, β_h)	0
(α_l, β_l)	2

Thus the data point for the utility curve will lie where $\alpha = \beta \rightarrow (\alpha, \beta)$ and therefore head down towards (0,0)

Graph

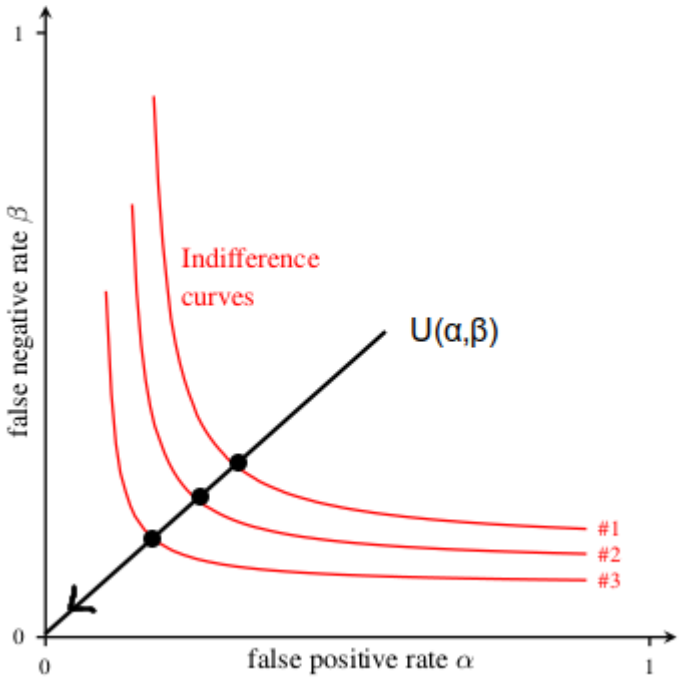
Thus lower the value of α and β gets, the greater the U gets. However we are indifferent between utility gained from α and β. The utility function is therefore:

$U(\alpha, \beta) = u \times \frac{1}{\alpha} + v \times \frac{1}{\beta}$

$u = v = 1$

$\therefore U(\alpha, \beta) = \frac{1}{\alpha} + \frac{1}{\beta}$

since the utility depends equally on both values, the graph for Utility curve would be:



c.

In this case the utility gained from limiting false positive is far greater than limiting false negative. This means we can trade off the high false negatives for lower false positives. Given assumption will be:

$(\alpha_l, \beta_h) \succ (\alpha_h, \beta_l)$

$(\alpha_l, \beta_l) \succ (\alpha_h, \beta_h)$

For ease of calculation I will assign:

$\alpha_h = -2$

$\alpha_l = 2$

$\beta_h = -1$

$\beta_l = 1$

Combination	Total Utility
(α_h, β_h)	-3
(α_h, β_l)	-1
(α_l, β_h)	1
(α_l, β_l)	3

The utility will depend on lowering α value, therefore the data point for utility will lie all on the lowest value of α on every indifference curve.

Graph

Above Utility Function can be expressed in general form:

$U(\alpha, \beta) = u \times \frac{1}{\alpha} + v \times \frac{1}{\beta}$

Because utility from lower α is the priority, we can assume that utility coming from β is low, and negligible.

$u > v$

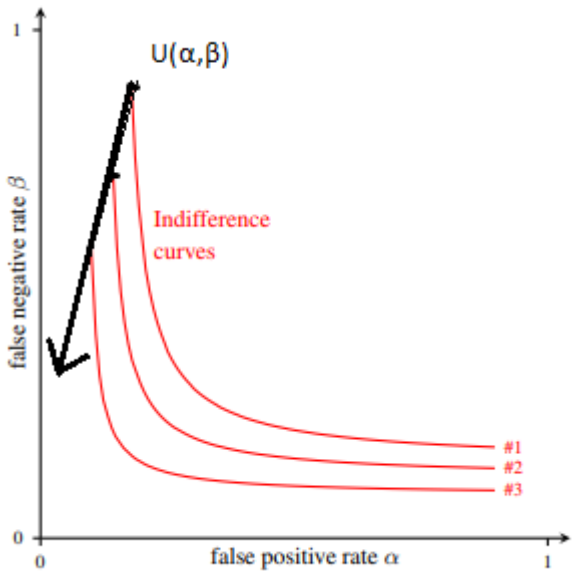
$u = 2$

$v = 0$

$U(\alpha, \beta) = 2 \times \frac{1}{\alpha} + 0 \times \frac{1}{\beta}$

$\therefore U(\alpha, \beta) = 2 \times \frac{1}{\alpha}$

since the utility solely depends on value of false positive, the graph would be:



Scenario 1

Trials in legal system. If we are sending people to jail, it would be more desirable to minimize the false positive - thus pro dubio reo.

Scenario 2

Interviewing process for Silicon Valley. If you are a firm hiring and you have enough talent applying, such as Google, the acceptance rate will decrease in order to make sure that you lower the chance of hiring an incompetent employee (false positives) even at the cost of missing some people who are good (false negative).

Q4

a.

$let\ |E(not)|\ = 0.01 \times \$5,000,000$

$let\ |E(do)|\ = \$25,000$

Since E(do) < E(not), it is more desirable to purchase the protection.

b.

$let\ |E(not)|\ = x \times \$5,000,000$

$let\ |E(do)|\ = \$25,000$

$x = \frac{\$25,000}{\$5,000,000} = \frac{1}{200} = 0.5\%$

As long as the probability of DDoS attack is greater than 0.5%, the company will justify paying for the protection

c.

Assumption 1. You assume that paying for protection will protect you 100% of the time. This is radically unreasonable as risk cannot be 0 in any situation.

Assumption 2. You assume that the payment for protection is one time. This is unreasonable because as of today there are no paid protection service that operates on single payment and continues to provide quality protection. If this company can, I want to question their profit model first.

Assumption 3. You assume that GoDaddy is risk neutral. I say this is justifiable because general corporations are risk neutral. Most corporations will take this approach because it yield them the most profit and does not discount, and firms exist to maximize profit.

Q5

1 We are spending enough money

In 2016, United State government $18,538,752 on cybersecurity [1]. Is this enough? The best way to see if you are spending enough money on something is to see if the job is being done. As president Obama has pointed out "So far, no one has managed to seriously damage or disrupt our critical infrastructure networks [2]." And this record continues despite many worries on U.S.'s cybersecurity. As one said, "no need to fix what ain't broken." We are doing enough for our protection.

Also, the U.S. government does not have to pay everything for protection of these infrastructures. The private sector has spent over $500 Billion [3], and the burden can be divided between private and public, and not fall completely on tax payer dollars.

2 We are not spending enough money

A quick math to determine if we are underspending the cybersecurity budget is to compare the risk to the cost.

$let\ E(damage)$ be dollar value of the market failure $\rightarrow$ failure of critical infrastructure

$let\ E(cost)$ be annual spending for protection of these critical infrastructure

$let\ P(damage)$ be probability of the market failure

$let\ x = \frac{E(damage)}{E(cost)}$ then,

$H_0 = E(damage) \times P(damage) \leq E(cost) \equiv x \geq P(damage)$

$H_a = E(damage) \times P(damage) > E(cost) \equiv x < P(damage)$

Null Hypothesis assumes we are spending enough on the cybersecurity.

For simplicity of mathematics, let's choose Nuclear Power Plant as an example. It is safe to assume that with the failure in nuclear power plant will at least result in the loss of the cost to build them. This amounts to $ 9,000,000,000 [4]. There are 61 commercially operating nuclear power plants in the United States [5].

$E(cost) = \$18,538,752$

$E(damage) = \$138,350,000,000$ [6]

Then, the threshold for the probability of damage in single power plant is:

$x = 0.000134 = 0.0134\%$

Since there are 61 power plants, this number becomes:

$x = 0.0000022 = 0.00022\%$

This is almost same number as the probability of 9/11 attack unfolding exactly as it did [7]. To assume that probability of breach in one of 61 nuclear power plants is lower than that of 9/11 is unreasonable. Moreover, this number is simply a calculation from nuclear power plants. We have many more infrastructures and their expected damage will only lower the threshold x. Therefore, it is reasonable to reject the null hypothesis and assume that we are not putting in enough funding for cybersecurity. In other words, the market is lacking willingness to pay.

The Market Failure thus comes from lack of demand. Government do not want to pay for the market price of cybersecurity because security naturally is a financial black hole. It does not yield money unless you are the supplier. For the infrastructures that already costs monstrously to build and maintain, it is reasonable for them to not want to pay any more than they already are paying.

3 My Choice

I personally agree with the 2nd view. The fact that private sector is spending increasing amount of money for cybersecurity is not something to be glad about, but it is a testimony that cyber attacks are getting harder to defend. While for any other product or service "don't fix what ain't broken" may hold, security is a different animal. Security serves as an insurance to some of the most important things in our society. The purpose of insurance is to convert risk to cost and have it be managed. Just because nothing has happened until now, does not mean it won't happen tomorrow.

SOURCE

[1] US spending on cybersecurity 2016

[2] President Obama's statement

[3] Private sector spending on Cybersecurity

[4] Cost of building nuclear power plants

[5] Nuclear power plant stats

[6] Cost of Accident

[7] 9/11 probability

Q6

Roughly 8 hours +. Admittedly a major portion of it was for formatting and editing. Q5 took a lot of time for me because I had to do separate research.