Discord risk management lifestyle

**Introduction**

With the continuous developments and renovations within technology, society has been able to expand the way in which education can be taught,understood and delivered to students. With the emergence of the internet students can access learning resources and materials from the comfort of their smart devices. One such platform that has made the learning experience more flexible for higher education students is learning management systems. Lms are platforms that enhance the collaboration between students and teachers by providing software based applications that can be interacted with and display data such as reports, progress and assignments.(Kasim, et,al 2016)

Over the years there have been many social media platforms introduced to the world as a means to communicate with friends and family and to share moments spent with them. However, higher education institutions have shifted the main purpose for these platforms and made use of their advantages to aid in the way in which they communicate and teach their students. One popular social media platform that is commonly used is discord. Discord a instant messaging platform where you can voice chat, send messages and share media contents between other users.(Schwartz,2021) With an estimated 250 million users, it is free to download and is compatible on everyday devices so anyone can join and collaborate ideas and projects. Originally meant for gaming, the services it provides have been expanded to allow for educational deliverance on their platform.

However with any application or social media platform, there will always be risks and vulnerabilities that can challenge the confidentiality, integrity and availability of the user. To understand what risks can be exploited by the social media platform, we first need to define and understand the meaning of risks. The definition of risk is a complex concept as it can vary depending on situations and circumstances. But in terms of this scenario, risk can be defined as the likelihood of an asset being attacked leaving financial,reputational and intellectual damage to a company or organization.(Ennouri,2013) There are many vulnerabilities that can increase the risk towards the discord platform. One common and well known example is a denial of service attack. This is where a server is flooded with millions of traffic that overwhelms the systems causing it to crash.(Sideleau.p, et.at,2005). This attack challenges the discord platform's availability as it prevents legitimate teachers and students from logging onto the platform. To combat these risks, we implement a risk management approach. Risk management can be defined as an approach to identify, assess, monitor and mitigate risks so that they have less of an impact on an organisation or companies resources and assets.(Dionne.G,2013). This report will be analysing the risks that are exposed to discord and assess those risks. To do this I will be using the Cobit 5 risk management lifecycle. The four stages of this lifecycle I will be exploring are: Risk identification,Risk assessment, Risk response and mitigation,Risk control monitoring and reporting. The stages will be used as guidelines to examine the risks and propose solutions to mitigate their exposure and as such, reduce their detrimental effect on assets.

**Risk management lifecycle**

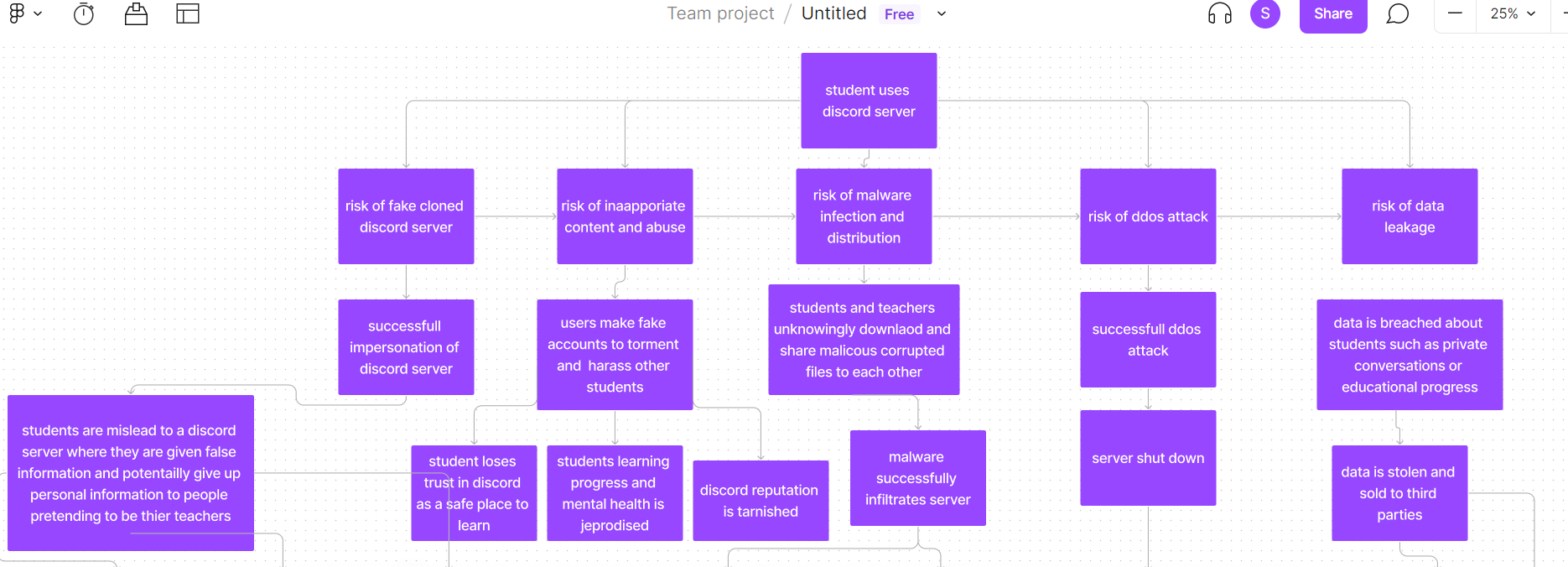
**Risk identification**

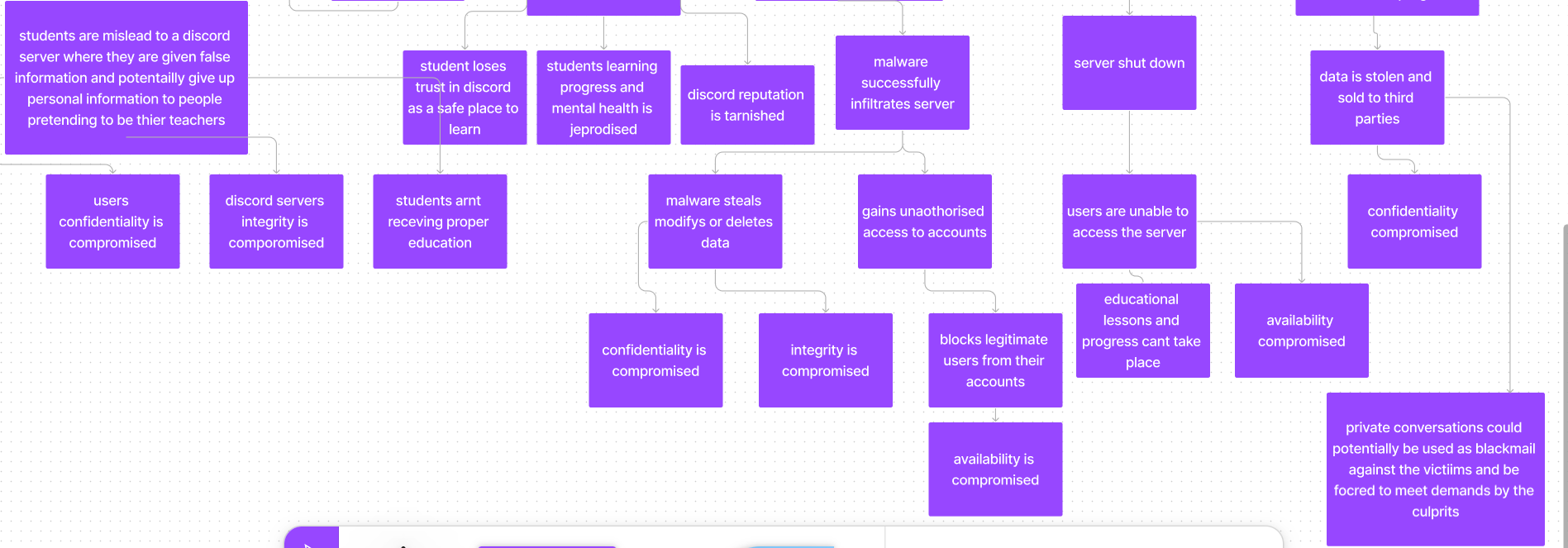
The first stage of the risk management lifecycle is risk identification. This is the stage where we identify any threats and vulnerabilities that can have a negative impact in regards to the assets held on discord. There are a collection of techniques and methods that can be utilised to understand the vulnerabilities within discord, their impact and their attack vectors. This is known as threat analysis. Within threat analysis there are two methods we can use, threat tree and attack tree.

**Threat trees**

Threat trees is a method used to visualise the different risks that are exposed to discord. The different threats and their impact are organised into a hierarchy to show how one action can lead to a certain result.

**Figure 1 threat tree to students using discord**

****

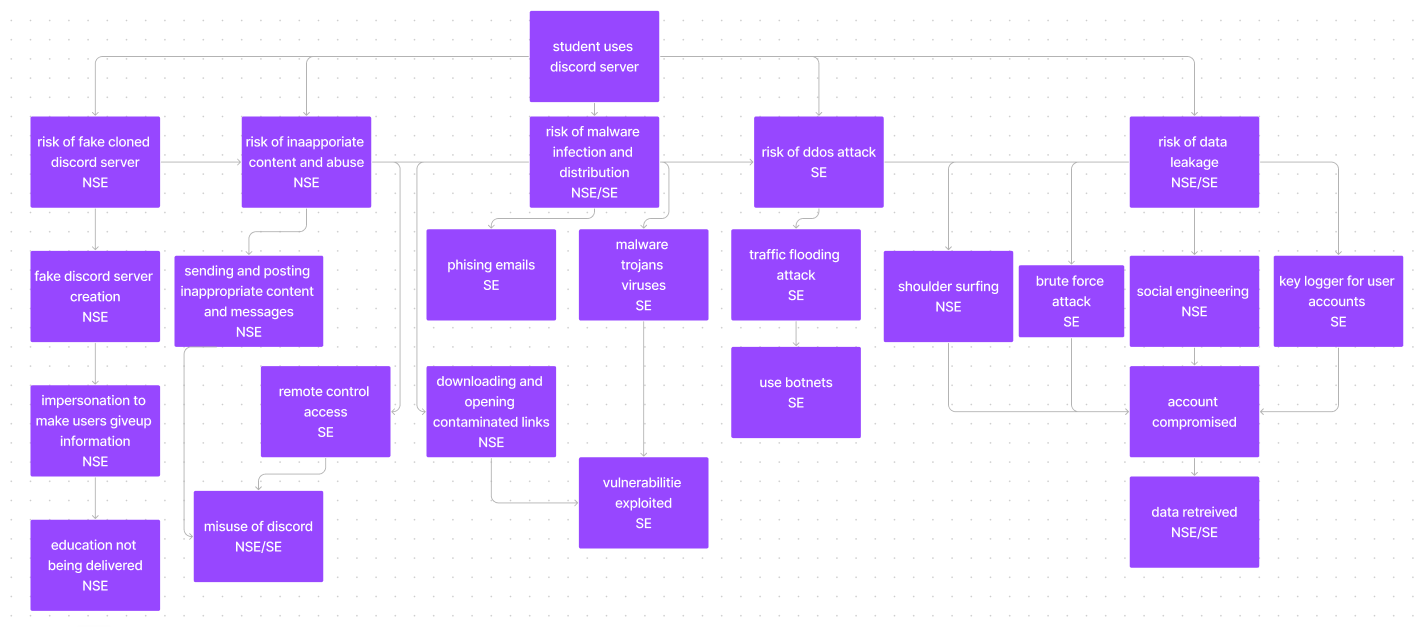
****

From the figure above, we can see how different risks that are exposed to discord can lead to several and severe consequences ranging from either reputational,financial, or mental. Whilst I only analysed five risks in detail, there are many more that can have damaging effects toward higher educational institutions.

**Attack trees**

Attack trees are another method of threat analysis that we can utilise. Attack trees show us from the attackers point of view, the different vectors that can be exploited. Furthermore, it informs us on whether specialised or unspecialised equipment is needed to perform the attack. This is again presented in a visual hierarchy.

**Figure 2 attack tree**



**Key**

**NSE= non specialised equipment**

**SE= specialised equipment**

From looking at the figure above, the attack tree demonstrates the different vectors that can lead to the above risks to take place. Within the attack tree it is shown whether specialised or non specialised equipment is required to perform the attack. In some instances, either type of equipment can be utilised. Through understanding and analysing the attack tree, we can use it as a blueprint to base any mitigation methods to prevent the risk from occurring.

**Risk assessment**

Risk assessment is the second stage of the risk management lifecycle. After the risks have been identified,it is important to analyse the impact the risks can have on a business or organization's assets.Furthermore, the risk assessment also analyses the likelihood of that risk occurring.From this information we can make decisions on which risk should be adhered to more. There are a number of methods we can use to undergo these analyses, either by using qualitative or quantitative methods.For this report I will be using both to assess the risks and their impacts on selected assets.

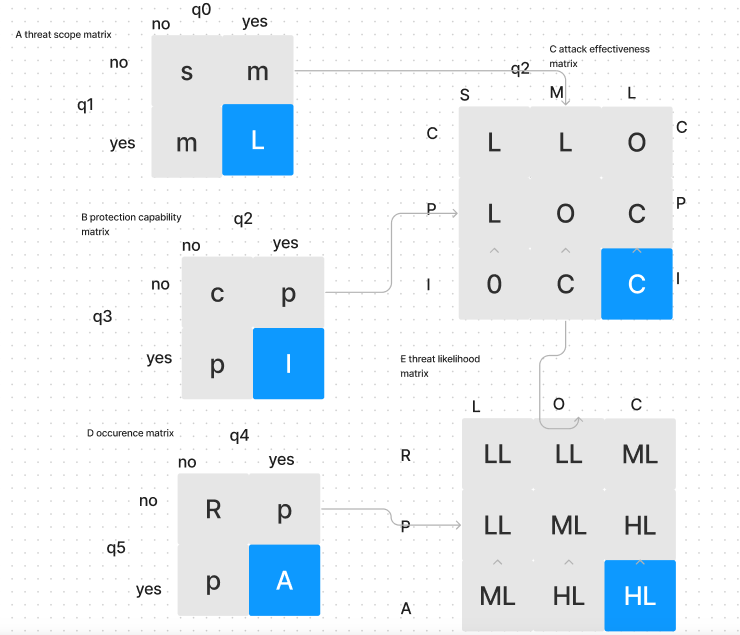
**Qualitative approach**

First I will start off with a qualitative methodology. Here I will use a binary risk assessment. This is where 10 questions will be asked against all the risks to give an estimated idea of the impact and likelihood of the specified risk. 4 of the questions are based on impact and 6 are based on likelihood. I will use either yes or no to answer the questions. After I will put this information into a matrix to get the impact,risk and likelihood of a risk.

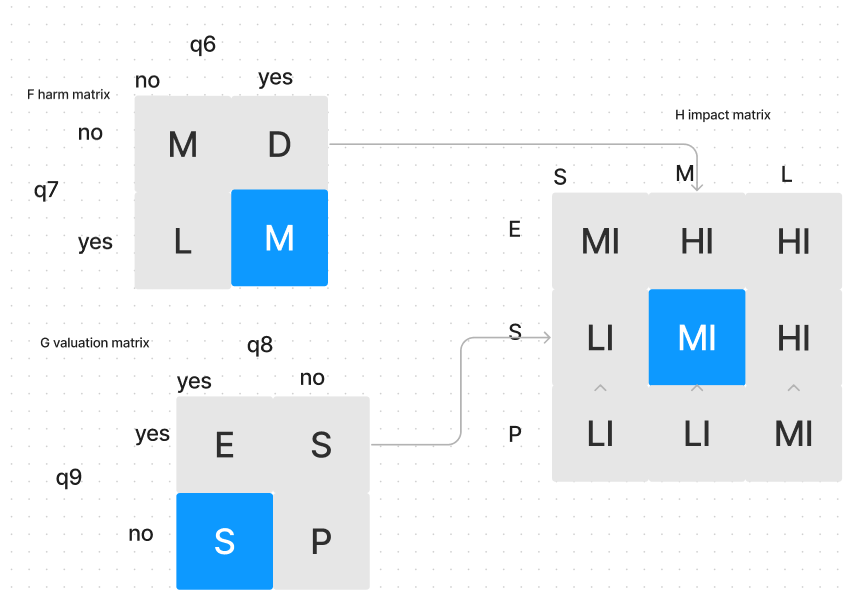
**Figure 3 BRA risk of fake cloned discord server**

| Question number | question | answer | rationale |
| --- | --- | --- | --- |
| 0 | Can the attack be completed with common skills? | Yes | Creating a fake discord server to imitate the real one can be done by anyone. Any individual can make one for free any clone the exact names,roles and descriptions of the original and send links to mislead users to join their server |
| 1 | Can the attack be completed without significant resources? | Yes | No special resources are required to make a fake discord server. All you need is a discord account which anyone can make for free in a small amount of time. |
| 2 | Is the asset undefended? | yes | There is no mechanism in place that can be used to identify if a server is a plagiarised version of a real one |
| 3 | Are there any weaknesses in the current defence? | Yes | Their is no verification to assess whether the owner of the server is who they claim to be and if the services they are hosting are genuine |
| 4 | Is the vulnerability always present in the asset? | yes | Cloning a server will always be possible at any given moment of the day |
| 5 | Can the attack be performed without meeting significant preconditions? | yes | No significant preconditions are needed. The only necessity would be knowing the structure of the server you are imitating which can easily be understood by joining the original server |
| 6 | Will there be consequences from internal sources? | yes | Students will be receiving false information and can give up personal information to fake teachers and instructors |
| 7 | Will there be consequences from external sources? | yes | The consequence from external sources can result in reputational and confidentiality issues for the institution |
| 8 | Does the asset have a significant business value? | yes | The server is the platform where education is delivered so if it is compromised then the proper education and communication cant be delivered |
| 9 | Will the asset have a significant cost of repair or replacement? | no | It doesn't cost money to make a server as its free but could take a long time to get all the material uploaded and ensure everyone has the right link |

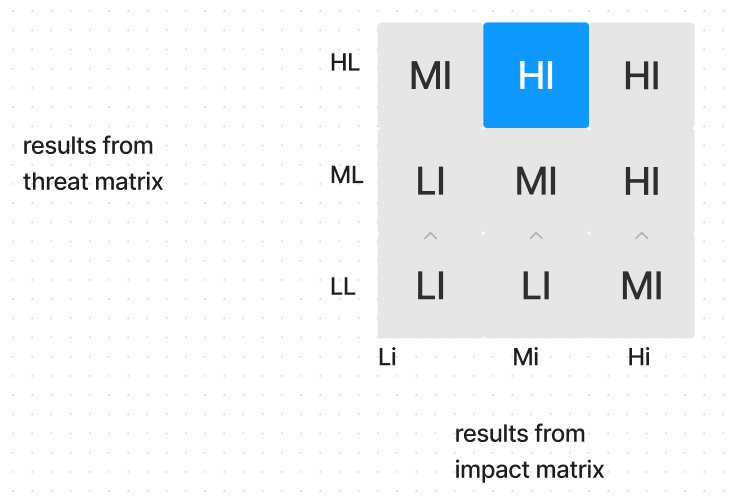
**Figure 4 determining likelihood**

****

**Figure 5 determining impact**

****

**Figure 6 determining risk**

****

**BRA results for risk of fake cloned server**

**LIKELIHOOD:** high likelihood

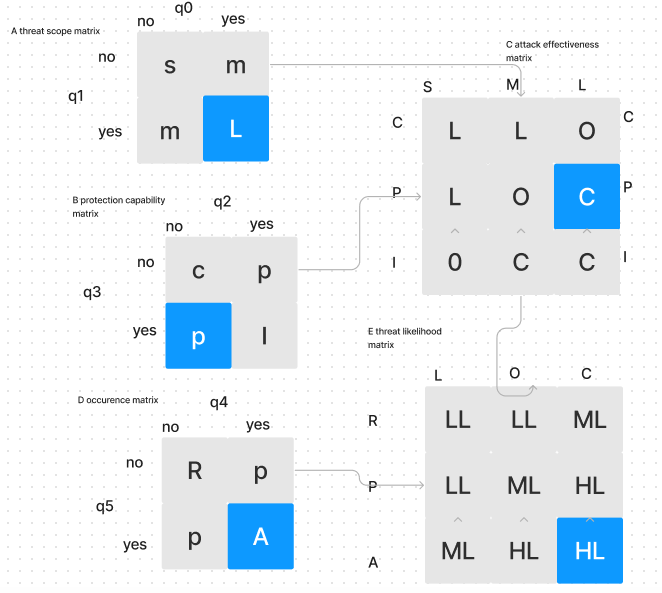
**IMPACT:** medium impact

**RISK:** high risk

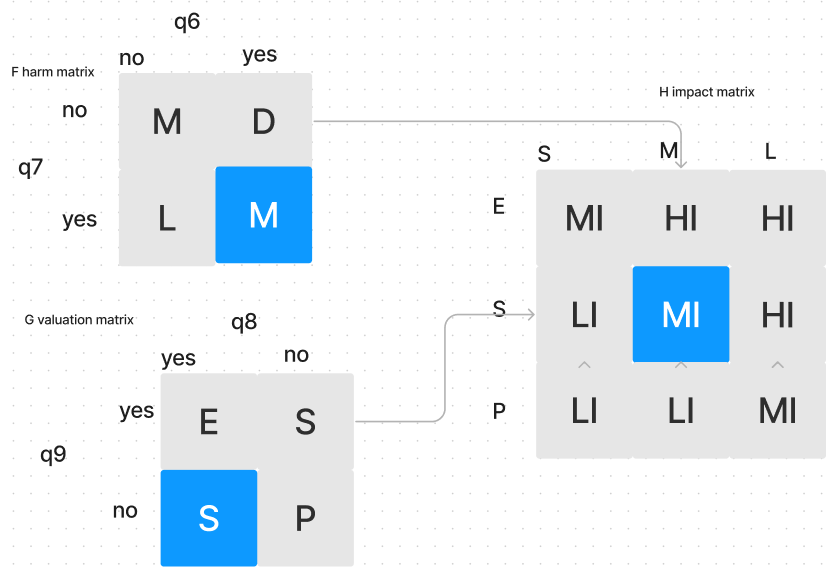
**Figure 7 BRA risk of inappropriate content and abuse**

| Question number | question | answer | rationale |
| --- | --- | --- | --- |
| 0 | Can the attack be completed with common skills? | yes | No special skills are needed to post and send harmful comments and images to users anyone is capable of doing it |
| 1 | Can the attack be completed without significant resources? | yes | No special resources are needed. The attack can be done as soon as you create a discord account |
| 2 | Is the asset undefended? | no | You can stop someone from sending you messages or content by switching your messages to only allow messages from friends that way only people you trust can contact you |
| 3 | Are there any weaknesses in the current defence? | yes | Harmful content and messages can be posted in general chats that everyone can see and view. There's no filter in place to stop these content and phrases from being sent |
| 4 | Is the vulnerability always present in the asset? | yes | Abusive language and context can always be sent to students at any time of the day |
| 5 | Can the attack be performed without meeting significant preconditions? | yes | The attack requires no significant preconditions as you can begin the attack as soon as you join a server or know someones username |
| 6 | Will there be consequences from internal sources? | yes | Students will be exposed to this abuse and have an effect on their mental health and as a result not be able to learn as productively as they would like to |
| 7 | Will there be consequences from external sources? | yes | The institution will be held accountable for the abuse and content with their reputation tarnished and possibly have to pay fines in compensation |
| 8 | Does the asset have a significant business value? | Yes | Chats and communication are what is utilised by discord if this is compromised then education can no longer be taught on the platform |
| 9 | Will the asset have a significant cost of repair or replacement? | no | It won't cost anything to remove the content or to ban the account soliciting the abuse.Howver there could be compensational and reputational costs along the way. |

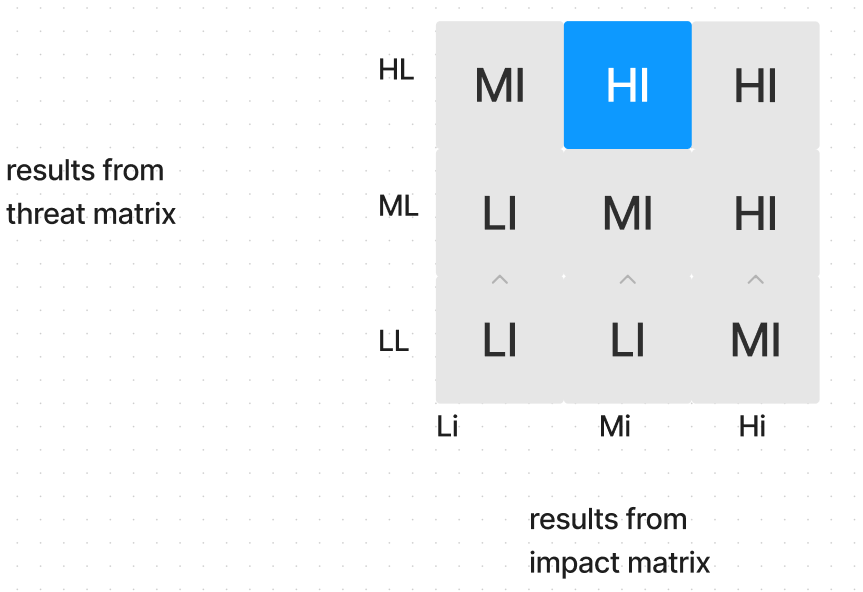
**Figure 8 determining likelihood**

****

**Figure 9 determining impact**

****

**Figure 10 determining risk**

****

**BRA results for risk of inappropriate content and abuse**

**LIKELIHOOD:** high likelihood

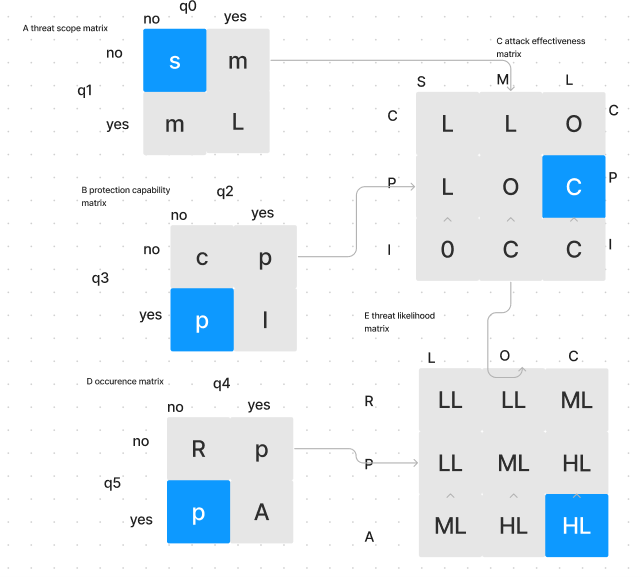
**IMPACT:** medium impact

**RISK:** high risk

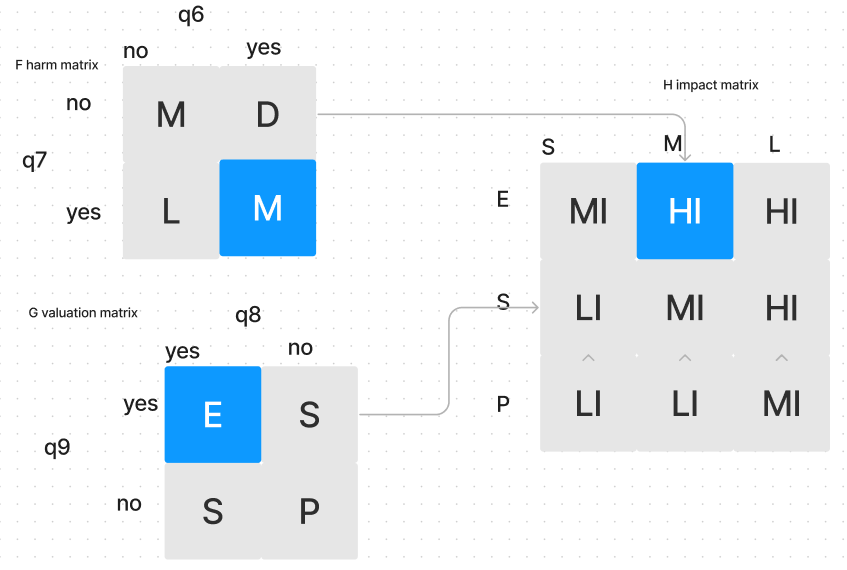
**Figure 11 BRA risk of malware infection and distribution**

| Question number | question | answer | rationale |
| --- | --- | --- | --- |
| 0 | Can the attack be completed with common skills? | no | Creating malware is something that would require practice and expertise that an average person wouldn't have |
| 1 | Can the attack be completed without significant resources? | no | Resources such as devices, software and botnets would be needed which wouldn't be easy to get a hold of |
| 2 | Is the asset undefended? | no | Discord would warn you before clicking a link which they believe is harmful,however some malware are still able to bypass it. |
| 3 | Are there any weaknesses in the current defence? | yes | Malware are able to distinguish themselves behind legitimate links and services which some of discords detection systems wouldn't pick up |
| 4 | Is the vulnerability always present in the asset? | yes | The malware can be within the system waiting to be initialised or spread to others |
| 5 | Can the attack be performed without meeting significant preconditions? | yes | The only precondition required would be making sure the malware does what its intended to do |
| 6 | Will there be consequences from internal sources? | yes | Students can unknowingly pass on and open the malware, this could lead to numerous events such as infecting their computer systems hijacking accounts and so on |
| 7 | Will there be consequences from external sources? | yes | The institution can be liable for damage costs to remove the malware |
| 8 | Does the asset have a significant business value? | yes | Discord server is where users communicate, if this is being used to facilitate malware then it can no longer be utilised |
| 9 | Will the asset have a significant cost of repair or replacement? | yes | Removing the malware from infected systems will take time money and expertise |

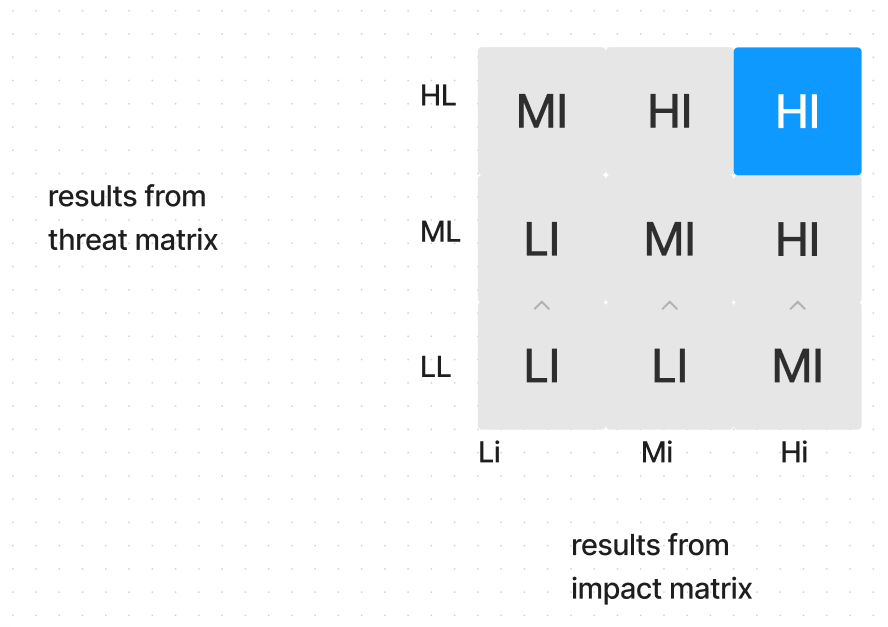
**Figure 12 determining likelihood**

****

**Figure 13 determining impact**

****

**Figure 14 determining risk**

****

**BRA results for risk of malware infection and distribution**

**LIKELIHOOD:** high likelihood

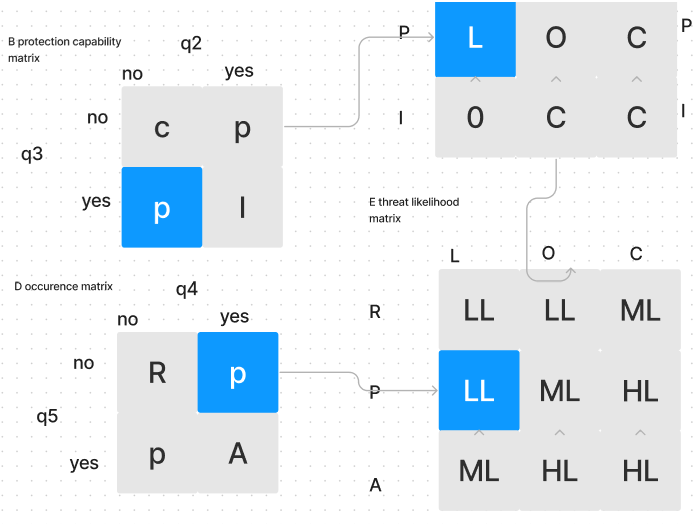
**IMPACT:** high impact

**RISK:**high risk

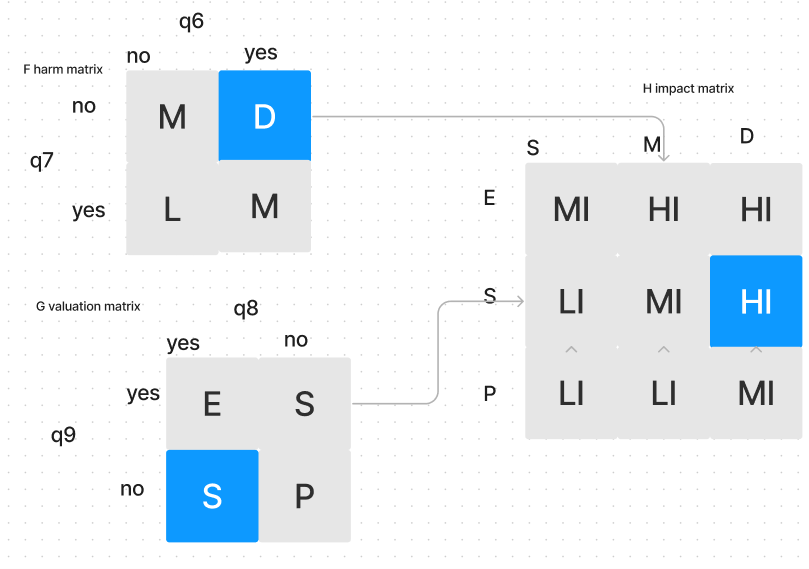
**Figure 15 BRA risk of ddos attack**

| Question number | question | answer | rationale |
| --- | --- | --- | --- |
| 0 | Can the attack be completed with common skills? | no | Performing a ddos attack will require skills and experience that the average person wouldn't be equipped with |
| 1 | Can the attack be completed without significant resources? | no | Ddos attacks will require a lot of computers within a network in order to send traffic. This can also be accompanied with botnets. These are significant resources themselves |
| 2 | Is the asset undefended? | no | There are mechanisms in place to prevent a ddos but any system can fall victim to it |
| 3 | Are there any weaknesses in the current defence? | yes | The servers can't handle massive influx of traffic unexpectedly |
| 4 | Is the vulnerability always present in the asset? | yes | A ddos can take place during anytime of the day |
| 5 | Can the attack be performed without meeting significant preconditions? | no | For a ddos to work all connected devices would have to send traffic at a predetermined time. |
| 6 | Will there be consequences from internal sources? | yes | Students and teachers will not be able to access discord as the servers will be down so eduction can be taught |
| 7 | Will there be consequences from external sources? | no | The person administering the attack is unlikely to get caught so there would be no legal action |
| 8 | Does the asset have a significant business value? | yes | Discord servers are pivotal in providing a platform that is flexible to be used for any type of service. If they are inaccessible then no productivity can be done. |
| 9 | Will the asset have a significant cost of repair or replacement? | no | Discord servers are free to create so no cost will be required the only downside is it will be time consuming. |

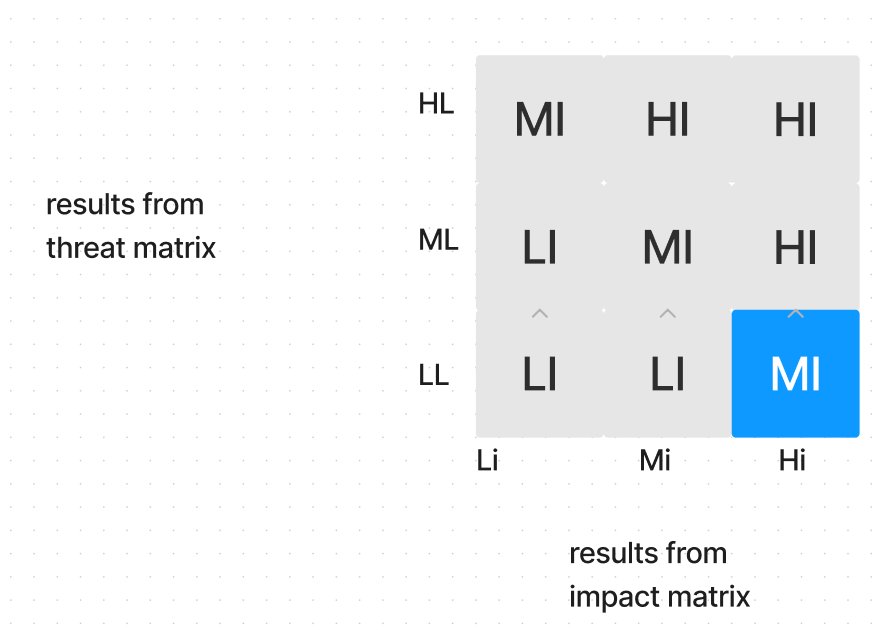
**Figure 16 determining likelihood**

****

**Figure 17 determining impact**

****

**Figure 18 determining risk**

****

**BRA results for risk of ddos attack**

**LIKELIHOOD:** low likelihood

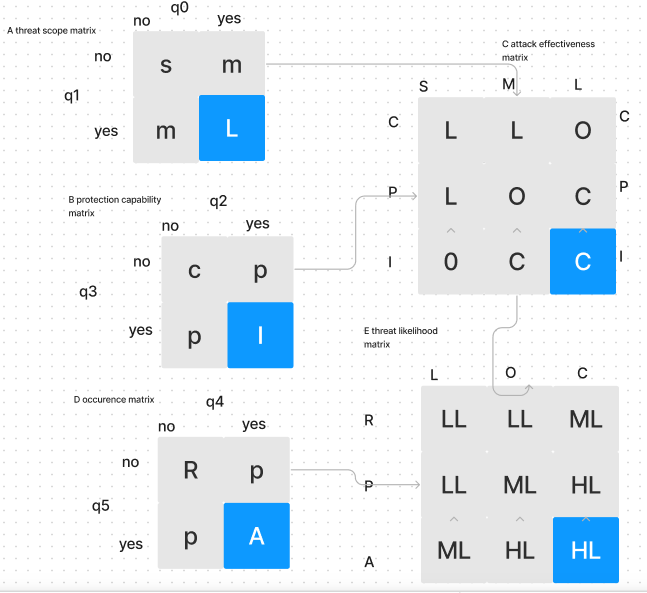
**IMPACT:** high impact

**RISK:** medium risk

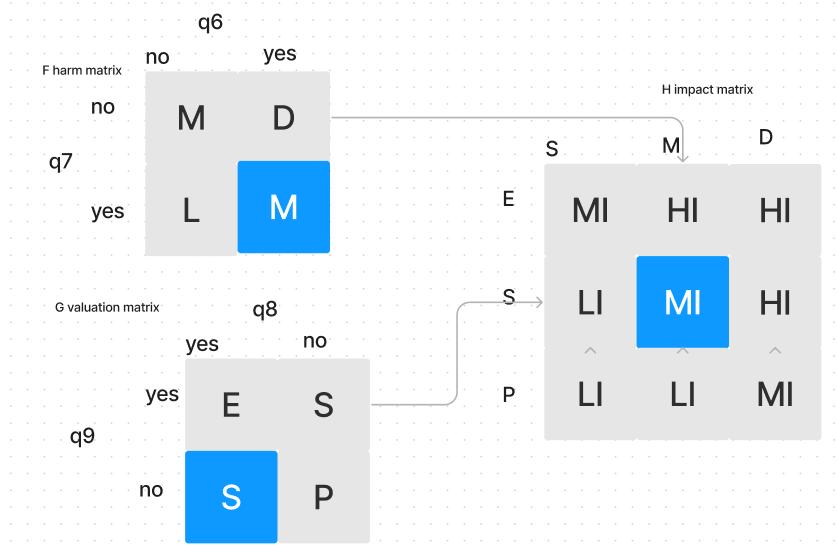
**Figure 16 BRA risk of data leakage**

| Question number | question | answer | rationale |
| --- | --- | --- | --- |
| 0 | Can the attack be completed with common skills? | yes | Techniques such as shoulder surfing or social engineering can easily be performed by the average person to gain confidential information |
| 1 | Can the attack be completed without significant resources? | yes | As long as you have a method of communicating with the target, that's all the resources needed |
| 2 | Is the asset undefended? | yes | There is no encryption mechanism in place to protect any communication or data that is exchanged |
| 3 | Are there any weaknesses in the current defence? | yes | Users are the greatest weakness as they are susceptible to social engineering and can be tricked by users pretending to be other students or teachers on the server |
| 4 | Is the vulnerability always present in the asset? | yes | Data being leaked will always be present either through the user or more specialised methods such as brute force |
| 5 | Can the attack be performed without meeting significant preconditions? | yes | The attack can be taken at any time without any preconditions |
| 6 | Will there be consequences from internal sources? | yes | The user who was targeted will suffer the consequences of the data leakage. |
| 7 | Will there be consequences from external sources? | yes | The reputation of discord would be challenged and users will lose trust in using the platform |
| 8 | Does the asset have a significant business value? | yes | Data within any organisation or business will be one of the biggest assets. If it is compromised then there would be huge consequences |
| 9 | Will the asset have a significant cost of repair or replacement? | no | Discord accounts and servers are free so no cost is needed to reinstate them however there could be compensation costs and damages to people's mental health |

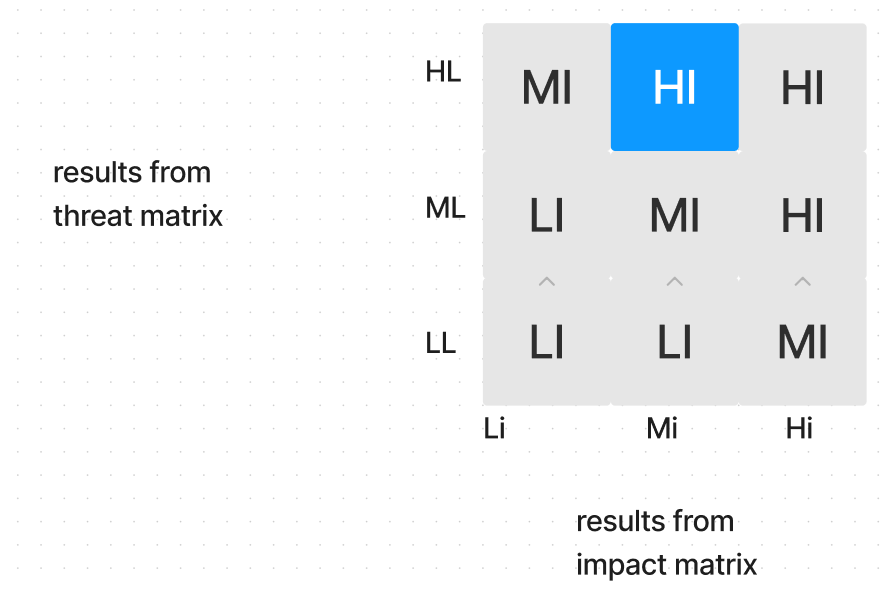
**Figure 17 determining likelihood**

****

**Figure 18 determining impact**

****

**Figure 19 determining risk**

****

**BRA results for risk of data leakage**

**LIKELIHOOD:** high likelihood

**IMPACT:** medium impact

**RISK:** high risk

**Quantitative approach**

The second approach is a quantitative method where I assess the impact a risk has in relation to an asset. I will be using a score system from 0 to 1. This will be used to score the risks for its likelihood,its impact, and the value an asset has towards the institution.

**Figure 20 quantitative table**

| asset/risks | Risk of fake cloned server  0.8 | Risk of inappropriate content and abuse  1 | Risk of malware infection and distribution  0.7 | Risk of ddos attack    0.7 | Risk of data leakage  1 | Total detrimental effect on asset |
| --- | --- | --- | --- | --- | --- | --- |
| Educational productivity 0.9 | 0.7  impact | 1  impact | 1  impact | 1  impact | 0.6  impact | 3.204 |
| Discord infrastructure 0..8 | 0  impact | 0  impact | 1  impact | 0.7  impact | 0  impact | 0.952 |
| Personal data 0.9 | 0.7  impact | 0  impact | 0.8  impact | 0  impact | 1  impact | 1.908 |
| Discord reputation 0.7 | 0.5  impact | 0.8  impact | 0.7  impact | 0.6  impact | 0.8  impact | 2.037 |
| Combined risk critically | 1.288 | 0.65 | 2.037 | 1.316 | 2 |  |

3.204= (0.8\*0.7)+(1\*1)+(0.7\*1)+(1\*0.7)+(1\*0.6)\*0.9

0.952=(0\*0.8)+(1\*0)+(0.7\*1)+(0.7\*0.7)+(1\*0)\*0.8

1.908=(0.7\*0.8)+(1\*0)+(0.7\*0.8)+(0.7\*0)+(1\*1)\*0.9

2.037=(0.8\*0.5)+(0.8\*1)+(0.7\*0.7)+(0.7\*0.6)+(1\*0.8)\*0.7

1.288=(0.9\*0.7)+(0.8\*0)+(0.9\*0.7)+(0.7\*0.5)\*0.8

0.65=(0.9\*1)+(0.8\*0)+(0.9\*0)+(0.7\*0.8)\*1

2.037=(0.9\*1)+(0.8\*1)+(0.9\*0.8)+(0.7\*0.7)\*0.7

2= (0.9\*0.6)+(0.8\*0)+(0.9\*1)+(0.7\*0.8)\*1

From assessing the table above we can see more specifically what risks are more prone to have a bigger effect on the selected asset. This can then be used as a starting point as to which asset should mitigation be focused on the most. From the data above I can come to the conclusion that malware distribution and infection is the biggest risk as it affects all assets the most. This would mean there should be heavy mitigation focus against this risk. Furthermore educational productivity is the most vulnerable asset so that should have increased procedures to protect it.

**Risk response and mitigation**

The next stage once the risks have been identified and assessed, is to implement methods and strategies so that the risks have a less detrimental effect on the assets and the institution. There are four different types of responses that are used in determining which approach would be best when mitigating the risk. I will outline them in the table below.

**Figure 21**

| Mitigation method | definition |
| --- | --- |
| Acceptance | A response where the organisation accepts the consequences of the risks.this could be due to the fact that the countermeasure costs more than the risk |
| transfer | Response where the risks is transferred from one department or organisation to another where it can be dealt with more effectively |
| mitigation | This is where countermeasures are implemented to reduce the risk,impact and likelihood of a selected risk |
| avoid | This is where an organisation attempts to ignore the risk all together either by using methods to prevent it from happening or reducing the likelihood |

**Risk countermeasure matrix**

A risk countermeasure matrix is a matrix that analyses the countermeasures effectiveness against reducing a risk that was identified during the risk assessment stage. The matrix will include the combined effect of the countermeasure against the risks and combined reduction. The higher the reduction value is for the countermeasure against the risk, the more effective it is.

**Figure 21 countermeasure matrix**

| countermeasure/risks | Risk of fake cloned server  0.8 | Risk of inappropriate content and abuse  1 | Risk of malware infection and distribution  0.7 | Risk of ddos attack    0.7 | Risk of data leakage  1 | Combined effect of countermeasure |
| --- | --- | --- | --- | --- | --- | --- |
| Content/keyword flagging AI  cost= 0.5 | Reduction =0 | reduction=1 | reduction=0 | reduction=0 | reduction=0 | 0.5 |
| Server authentication protocol cost =0.4 | reduction=0.9 | reduction=0 | reduction=0.4 | reduction=0 | reduction=0.7 | 0.68 |
| Anti malware system  Cost = 0.3 | reduction=0 | reduction=0 | reduction=1 | reduction=0.3 | reduction=0.5 | 0.099 |
| Firewall cost = 0.5 | reduction=0 | reduction=0 | reduction=0.8 | reduction=1 | reduction=0 | 0.63 |
| Social engineering warnings/ bulletins  Cost = 0.1 | reduction=0 | reduction=0.1 | reduction=0.6 | reduction-0 | reduction=0.7 | 0.01 |
| Combined risk reduction | 0.288 | 0.051 | 0.644 | 0.483 | 0.5 |  |
|  |  |  |  |  |  |  |

0.5=(0.8\*0)+(1\*1)+(0.7\*0)+(0.7\*0)+(1\*0)\*0.5

0.68=(0.8\*0.9)+(1\*0)+(0.7\*0.4)+(0.7\*0)+(1\*0.7)\*0.4

0.099=(0.8\*0)+(0\*1)+(0.7\*1)+(0.7\*0.3)+(1\*0.5)\*0.3

0.63=(0\*0.8)+(1\*0.1)+(0\*0.6)+(0\*0)+(0\*0.7)\*0.5

0.01=(0\*8)+(1\*0.1)+(0\*0.6)+(0\*0)+(0\*0.7)\*0.1

0.288=(0.5\*0)+(0.4\*0.9)+(0.3\*0)+(0.5\*0)+(0.1\*0)\*0.8

0.051=(0.5\*1)+(0.4\*0)+(0.3\*0)+(0.5\*0)+(0.1\*0.1)\*1

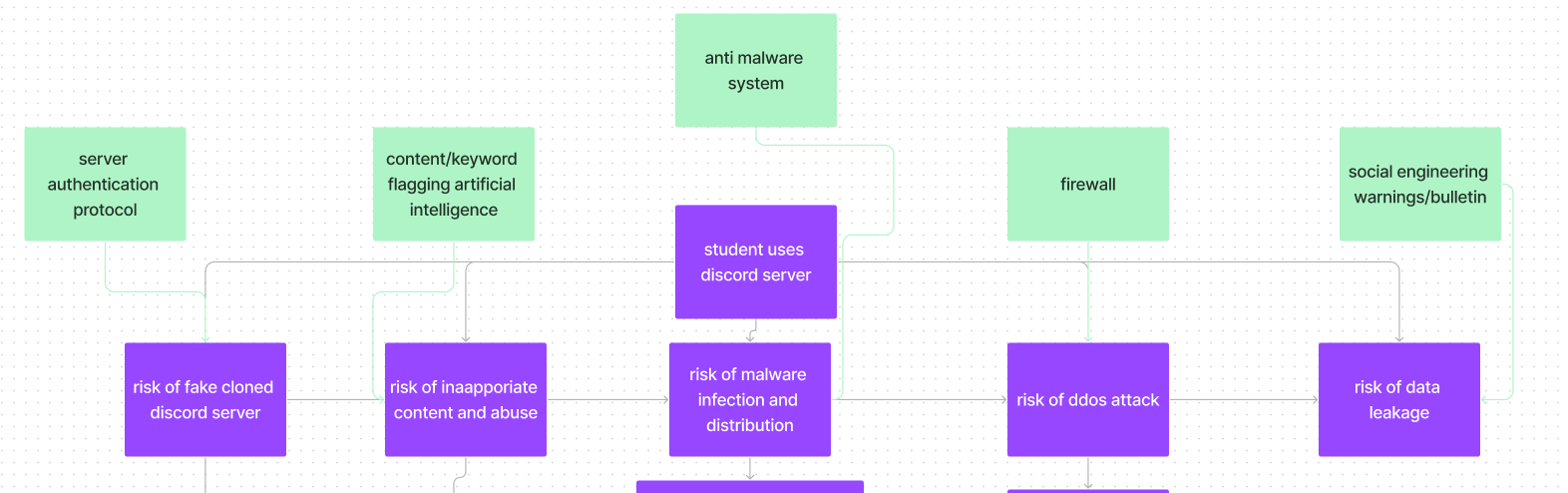
0.644=(0.5\*0)+(0.4\*0.4)+(0.3\*1)+(0.5\*0.8)+(0.1\*0.6)\*0.7

0.483=(0.5\*0)+(0.4\*0)+(0.3\*0.3)+(0.5\*1)+(0.1\*1)\*0.7

0.5=(0.5\*0)+(0.4\*0.7)+(0.3\*0.5)+(0.5\*0)+(0.1\*0.7)\*1

From analysing the data above we can see that a server authentication protocol has the greatest combined countermeasure across all the countermeasures. This would imply that this countermeasure would be the best to implement, however it should be taken into consideration that not all countermeasures deal with all the risks as effectively as we would like. Furthermore, the table above shows us that the risk of malware is most dealt with against all the countermeasures.

**Figure 22 risks with countermeasures**



Above is a figure that shows what countermeasures correspond with what risk.

**Risk control monitoring and report**

The last stage of the life cycle, risk control and monitoring, is where we monitor all present or potential risks including those that were introduced by implementing the countermeasures. This is a crucial stage as the organisation uses this information to plan how they will move forward. Monitoring can be achieved through either software such as ids or ips or manually through using a matrix or KRI’S. I will be proposing several kris and discussing their relevance.

**Malware indicator**

(Number of malware detected/number of malware quarantined)\*100

This indicator calculates the total amount of malware detected and divides it against how many were quarantined. This indicator is relevant as on discord, numerous malware can be running across servers. Having statistical data on how effective they are being handled would help in deciding if more malware detection systems need to be introduced.

**Inappropriate content indicator**

**(**number of indecent content/ messages reported**/**number of indecent content/messages removed**)\***100

This indicator calculates the total number of indecent messages and content reported and divides by the total number that is removed. This indicator is relevant as we can see if the artificial intelligence is effective when dealing with the flagged content. This is imperative so that students' mental wellbeing isn't being threatened by trolls or other students.

**Fake discord server indicator**

(time fake server is created-time fake server is removed)/total number of fake servers

This indicator calculates the time it takes for a fake server to get removed. This is relevant as fake servers can be created at any moment. To ensure they are flagged and removed quickly, it is imperative that we have an understanding of how fast the response is in shutting them down.

**Conclusion**

This report has analysed discord as a social media platform for learning and discussed the risks and mitigation methods for those risks in correlation with the risk assessment lifestyle methodology. I have used both quantitative and qualitative methods to analyse the risks along with their impacts towards the higher institution in terms of education being delivered. Whilst only 5 risks when analysed, more can be looked at in more detail to add more insight and knowledge into what discord is exposed to and how they can be counteracted.

It is necessary for the risk assessment lifecycle to be continually implemented so that a higher institution can regularly update their awareness on what assets are at risk, what new or old risks are prevalent and whether or not the countermeasures are having a positive effect in combating them.

Discord is a social media platform that has been used more recently for educational purposes. It has become more popular over the years and used by all sorts of organizations.With any social media platform or application, there will always be risks and vulnerabilities that can be taken advantage of. To reduce the problems it is beneficial to have regular monitoring and protocols so that an organisation's understanding is continually being broadened.

References

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk management and insurance review*, *16*(2), 147-166. [Risk Management: History, Definition, and Critique - Dionne - 2013 - Risk Management and Insurance Review - Wiley Online Library](https://onlinelibrary.wiley.com/doi/full/10.1111/rmir.12016?casa_token=5ki5zIgYU_UAAAAA%3AO6JkfA9CibEUbM4HPGwN66yJAFZhGh353NfdrBWZ1FtkjRAdgevvkbYWSim055ZwPgE3VBj3KDlfp54)

["Denial of Service Attack Techniques: Analysis, Implementation and Comp" by Khaled M. Elleithy, Drazen Blagovic et al. (sacredheart.edu)](https://digitalcommons.sacredheart.edu/computersci_fac/52/)

Elleithy, K. M., Blagovic, D., Cheng, W. K., & Sideleau, P. (2005). Denial of service attack techniques: analysis, implementation and comparison.

[d35a18c9-c3ce-31be-8f0a-473b92793a66 (infona.pl)](https://www.infona.pl/resource/bwmeta1.element.baztech-c18616d2-64b5-417e-9a5a-5cfcbdeecb9e/content/partContents/d35a18c9-c3ce-31be-8f0a-473b92793a66) Ennouri, W. (2013). Risks management: new literature review. *Polish journal of management studies*, *8*, 288-297.

[Using Discord to Facilitate Student Engagement (unlv.edu)](https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1122&context=btp_expo) Schwartz, D. (2021). Using Discord to facilitate student engagement.

Kasim, N. N. M., & Khalid, F. (2016). Choosing the right learning management system (LMS) for the higher education institution context: A systematic review. *International Journal of Emerging Technologies in Learning*, *11*(6). [Choosing-the-Right-Learning-Management-System-LMS-for-the-Higher-Education-Institution-Context-A-Systematic-Review.pdf (researchgate.net)](https://www.researchgate.net/profile/Fariza-Khalid/publication/304527983_Choosing_the_Right_Learning_Management_System_LMS_for_the_Higher_Education_Institution_Context_A_Systematic_Review/links/5782f4b608ae5f367d3b680d/Choosing-the-Right-Learning-Management-System-LMS-for-the-Higher-Education-Institution-Context-A-Systematic-Review.pdf)