[DRAFT] Underground Markets: Security and Risk Management

WM0824TU Economics of Cyber Security - Group 16
September 30, 2019

Name	Student Number
Veroniek Binkhorst	4276620
Rowdy Chotkan	4570243
Björn Ho	4320867
Swaathi Vetrivel	4900863

Table of Contents

1. Introduction

<will be added in the final version>

2. Problem Owner

The issue identified in block 2 is defined as: *"The socio-economic impact on society caused by underground markets that facilitate cybercrime"* . The main actor trying to decrease this impact was identified as the law enforcement agencies (LEAs). In this report, we further narrow down this actor to the relative governmental department that handles these issues and, hence, can be described as the problem owner. In particular, we focus on the US with the FBI's Cyber Division (CyD), which combats cybercrime[1]. This actor has been selected since this party has the resources, institutional power, and motive to mitigate the security issue and the risks it facilitates.

The video lectures given by Böhme discuss four different actors in the cybersecurity industry. These being:

- Security "providers"
- Security "consumers"
- Security industry
- Attackers

FBI's Cyber Division can be translated to the "security providers" category, since they are in the position of being able to shape the information security environment, as defined by Böhme.

3. Security Performance

For understanding the security performance of CyD, we can use the performance measure published by the FBI in their annual financial statements. The FBI measures and tracks the performance of the CyD using the performance metric "*Number of Computer Intrusion Program Disruptions and Dismantlements*". This performance measure is intended to capture the operational capability of the CyD to interrupt and eliminate cyber actors from engaging in cybercrime activities.

CyD manages computer intrusion and dismantlement operations to eliminate the intrusion capabilities of threat enterprises and organizations. These operations are classified into four types - deterrence, detection, disruption and dismantlement. Detection is identification of threats to national security related activity and deterrence is the prevention of these threats through defensive countermeasures. Disruptions inhibit the threat actor's activities through actions like arrest or seizure of assets. Dismantlement is when the targeted organization's leadership or network has been destroyed in such a way that the organization is incapable of reforming itself.

[1] https://www.fbi.gov/investigate/cyber

To compare the performance of the CyD over different time periods, financial statements from the years 2014 (the year the measure was implemented) to 2018 (the last available year) was examined, the relevant details are captured in the table below[2].

	Number of Computer Intrusion Program Disruptions and Dismantlements				*Number of computer intrusion program, deterrences, detections, disruptions and dismantlements*
	2014	**2015**	**2016**	**2017**	**2018**
Target	100	500	500	500	4200
Actual Performance	2492	479	250	262	11540

Analysis of the measure across these years shows that the initial target of 100 disruptions and dismantlement was increased to 500 in 2015 and remained constant till 2017. In 2014, the actual performance was 2492 against the target of 100. In the subsequent years between 2015 and 2017, the actual performance was 479, 250 and 262 respectively.
In 2018, the measure was broadened to include deterrence and detection in addition to disruption and dismantlement. With this measure, the target in 2018 was increased to 4200 although the actual performance in this period was 11540 which almost three times as much. This dramatic increase in the number of operations can be accounted for the enhancement of the metric to include additional operations.

Although this measure offers a metric to track the CyD's performance, it does not offer information on the total number of cyber threats identified nor does it capture the magnitude of the threats that were prevented.

Global CyberSecurity Index

To capture the security performance of different countries we use the Global CyberSecurity Index[3]. The Global Cybersecurity Index (GCI) is a project of the International Telecommunication Union to rank the cybersecurity capabilities of nation states. This index captures the commitment of member states towards cybersecurity at a global level. Each country's level of development or engagement is assessed along the following five pillars and then aggregated into an overall score
(i) Legal Measures

[2] https://www.oversight.gov/report/doj/audit-federal-bureau-investigation-annual-financial-statements-fiscal-year-2014
https://www.oversight.gov/report/doj/audit-federal-bureau-investigation-annual-financial-statements-fiscal-year-2015
https://www.oversight.gov/report/doj/audit-federal-bureau-investigation-annual-financial-statements-fiscal-year-2016
https://www.oversight.gov/report/doj/audit-federal-bureau-investigation-annual-financial-statements-fiscal-year-2017
https://www.oversight.gov/report/doj/audit-federal-bureau-investigation-annual-financial-statements-fiscal-year-2018

[3] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

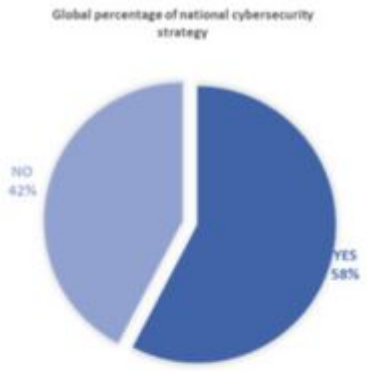
(ii) Technical Measures
(iii) Organizational Measures
(iv) Capacity Building
(v) Cooperation
Global Commitment Level
The most committed countries globally in 2018 are captured in the following table.

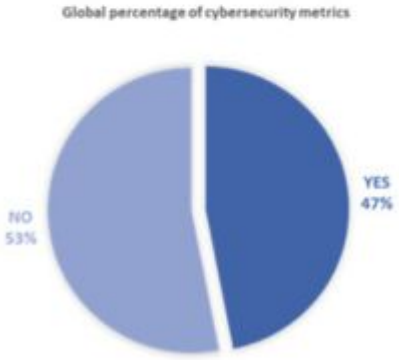
Rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
2	United States of America	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
10	Canada	0.892	0.195	0.189	0.200	0.172	0.137
11	Australia	0.890	0.200	0.174	0.200	0.176	0.139

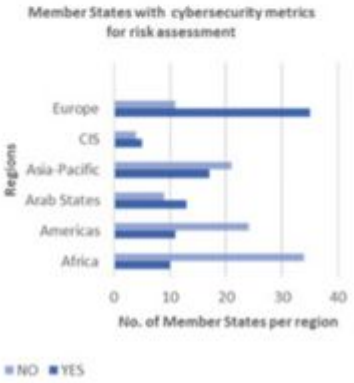
This table shows that the top 11 countries come from only three regions of ITU six countries from the Europe region, three from the Asia-Pacific region, and two from the Americas region. This reflects the wide gap in cyber commitment around the world.

National cybersecurity strategy and cybersecurity metrics globally and per region

Another insightful indicator captured by the GCI is a comparison of cyber security strategy and metrics availability across countries. The results are captured below.







This shows that there is room for improvement since performance measurement is a key aspect of cybersecurity risk management. Cybersecurity governance and risk management that allows for development, implementation, monitoring and updation of metrics that provide visibility on the performance of key elements of a national cybersecurity program would help with measuring the performance of the countries against cyber risks and threats.

4. Risk Strategies

In order to develop risk strategies, it is essential to first perform a systematic analysis of the risk raised due to various activities in the underground markets and perform a risk assessment. Within formal risk management framework, risk assessment is described as the process of identifying, characterizing, and understanding risk; where risk is defined as a set of outcomes and associated likelihoods of occurrence. After the risks are quantified, alternative strategies to deal with the risks can be identified and decisions about acceptable risk level can be made. Cost-benefit calculations, assessments of risk tolerance, and quantification of preferences can help estimate the effects of the identified strategies on risk reduction, elimination or reallocation (Soo Hoo, 2000). The strategies to deal with risk can be towards risk mitigation, acceptance, transfer or avoidance.

Risk mitigation

The risks that are deemed to be high should be mitigated to decrease the likelihood and the severity of loss events. Thus, a mitigation strategy for CyD should aim to both reduce the activity in the underground market and decrease the consequent socio-economic impact on society from the activity. The deterrence, detection, disruption and dismantlement operations described in section 3 are part of CyD's mitigation strategy. In addition, CyD could employ the following strategies.

1. The servers of the underground markets that show the highest amount of activity and turnover could be tracked down and decommissioned from service.
2. Most users of underground markets use tools like TOR for anonymity. Passing laws that ban the use of TOR might be helpful in restricting access to these marketplaces.
3. Increasing awareness about cybercrime amongst the general public and educating them on best security practices to avoid being targeted will help in decreasing the impact the underground market activities have on society.
4. The vulnerabilities exploited by the items offered for sale in the underground markets can be assessed and mitigated through corresponding vulnerability mitigation strategies.
5. Stricter cybersecurity policies can be mandated for both software and hardware. For instance, making AES-128 compulsory might eliminate vulnerabilities arising from using older security protocols.

Risk acceptance

Irrespective of the amount of risk mitigation strategies employed, there are bound to be residual risks that cannot be prevented. Moreover, there might be threats that are deemed low risk and offer low benefits for the costs involved. CyD could choose to accept these risks and ensure these are catalogued and monitored periodically to ascertain that the associated risk level does not change. The accepted risks that materialize need to be managed through appropriate incident management and response activities. These include communication about the incident to the stakeholders, ensuring the threat is contained, repairing the

damages caused and conducting postmortem analysis of the event to better manage future threats.

Risk transfer

Some risks might not be low enough to be accepted but CyD might not be best positioned to mitigate the risk. This could arise because it has a lack of resources, expertise and specialization to deal with them. These risks could be transferred to other establishments that have sufficient resources available. One possible strategy would be inter-agency collaboration (i.e) collaboration with other local and international law enforcement agencies to share information about the suspected threats and the associated risk level. Alternately, CyD could also choose to collaborate with the private sector directly by sharing information that would enable them to better protect themselves against the risk. For instance, if a particular industry like the financial sector is being targeted, information sharing with members of the financial sector would facilitate intra-organizational security cooperation within the sector and allow for collective resources of the financial sector to be employed in defending against the risk. Further, CyD could hold the responsible companies liable for the risks exposed by their activities which would incentivise the companies to adopt better security practices. For instance, credit card companies can be made liable for the risk associated with fraudulent credit card transactions due to information leakage in the underground markets. This would offer the credit card companies incentive to protect against such casualties and push them to follow a stricter cybersecurity policy.

Risk avoidance

Risk avoidance strategies aim to eliminate exposure to risk entirely. While the risk from underground markets cannot be avoided altogether, some threats can be avoided by better security management and adherence to security frameworks by the responsible parties. CyD could work with the government to pass laws that incentivise the private sector to install safeguards in their systems to avoid the threats. For instance, a law that mandates that all systems should be updated with the latest security patches will help avoid risks that arise due to older vulnerabilities.

5. Actors' influence, incentives, and strategies

In this section it will be discussed which other actors can influence the socio-economic impact on society caused by underground markets that facilitate cybercrime. For each actor their possible strategies will be discussed, as well as their incentives to act or not to act. Based on their incentives, their interest in reducing the socio-economic impact on society caused by underground markets that facilitate cybercrime is the security issue will be scored as high, medium or low.

5.1 Users of the platforms

The users of the platform are the reason the platform exist. Without buyers there wouldn't be any sellers, and without sellers there wouldn't be any buyers. The users however do not have enough incentives to stop using the platform, mainly because the sellers earn money, the buyers are able to buy the product they want to buy, and the chance the buyers or sellers get caught and sentenced for their actions are slim.Therefore, the users of the platforms interest to reduce socio-economic impact on society caused by underground markets that facilitate cybercrime is scored as low.

5.2 Users of IoT devices

The users of IoT devices are the owners of those devices and thus have influence regarding the security of their devices. A strategy they can implement is securing their devices, by for example installing antivirus. by installing antivirus their data is protected and more difficult to steal and they can prevent their machines from becoming part of a botnet.

Van Eeten & Bauer (2009) describe three reasons why users of IoT devices have little incentive to act upon the security issue. First of all, malware is increasingly designed to have as little impact as possible on the infected device, therefore it does not affect the users of IoT devices individually. The second reason is because users of IoT devices might not be aware their machine is infected. Third, because many financial service providers offer compensation for losses incurred by their customers, this disincentivize customers to be as secure as possible when dealing with their financial data. Because of these reasons, the users of IoT devices interest to reduce socio-economic impact on society caused by underground markets that facilitate cybercrime is scored as low.

5.3 Internet Service Providers

The internet Service Providers (ISPs) are intermediaries that make it possible for users to access the internet and also to access black markets. The ISPs role is twofold: they themselves are impacted by underground markets that facilitate cybercrime and they also facilitate the existence of these underground markets. For the security issue, their role as facilitators is interesting and their role as victim is not, unless strategies focused on their role as victim also affect their role as facilitator.

To understand the influence of the ISPs and the risk strategies they can adopt to tackle the problem, it is important to understand the incentives of the ISPs to act or not to act against underground markets. Most ISPs are increasing their efforts to fight malware, for which multiple reasons are given in the article of Van Eeten & Bauer (2009). The reasons include the costs of customer support and abuse management, the costs of blacklisting, the costs of brand damage and reputation effects, the costs of infrastructure expansion, and the benefits of maintaining reciprocity within the ISP's network. The disincentives include the legal risks and constraints and cost of customer acquisition. Because ISPs are increasing their effort and do have incentives to do so, but also have incentives to not act, their interest to reduce

socio-economic impact on society caused by underground markets that facilitate cybercrime is scored as medium.

Since the ISPs are an intermediary party, they have a lot of strategies to mitigate the socio-economic impact on society caused by underground markets that facilitate cybercrime:

1. Increase customer awareness for the need for secure practices. Increasing awareness can result in more secure practices by customers, which in turn will lead to less security incidents and less customers contacting ISPs with questions related to security incidents. More secure practices will also lead to less possibilities for devices being used for for example DDoS attacks, thus resulting in less traffic on the network.
2. Offering security software for free with subscription (Van Eeten & Bauer, 2009). This has the same effect as increasing customer awareness and will result in less customers contacting ISPs with questions related to security incidents and less traffic on the network.
3. Offering free filtering of email with subscription (Van Eeten & Bauer, 2009). This also has the same effect as increasing customer awareness and will result in less customers contacting ISPs with questions related to security incidents and less traffic on the network.
4. ISPs can pressure other ISPs to take action by for example threatening to blacklist all or part of their IP addresses. This is undesirable for ISPs because it makes them less attractive to customers.
5. ISPs can communicate with each other and other parties in their network and in this way work together to act on a case of abuse.
6. ISPs can choose to not allow the user onto the TOR network. Whether this is possible depends on countries laws and regulations however, because for example of the EU E-commerce Directe which ensures net neutrality.

5.4 Security Vendors

Security vendors can increase the security defences of their products, but because they are a business that wants to maximize their profit, they have an incentive not to do so if it is not economically efficient anymore. Because of this reason, their interest to reduce socio-economic impact on society caused by underground markets that facilitate cybercrime is scored as low.

5.5 Law enforcement from other countries

Law enforcement agencies want to stop underground markets from operating, because of violation of the law and the impact they have on society. Therefore, their interest to reduce socio-economic impact on society caused by underground markets that facilitate cybercrime is scored as high.

On 3 May 2019 Europol made a press release available named “Double blow to dark web marketplaces” (Europol, 2019). According to this press release, The German Federal Criminal Police (Bundeskriminalamt) shut down the Wall Street Market, under the authority

of the German Public Prosecutor's office. To be able to do so, they were supported by the Dutch National Police (Politie), Europol, Eurojust and various US government agencies (Drug Enforcement Administration, Federal Bureau of Investigation, Internal Revenue Service, Homeland Security Investigations, US Postal Inspection Service, and the US Department of Justice). This is an example of how law enforcement can work together on a coordinated approach to reduce the socio-economic impact on society caused by underground markets that facilitate cybercrime. Out of this coordinated approach three strategies can be formed.

1. Law enforcements can work together by sharing information regarding knowledge about the physical location of a server which hosts a black market. By sharing this information, the local law enforcement agency can take down a black market.
2. Law enforcement can also work together by sharing information regarding knowledge about 'big fish' and in this way take out big sellers on a black market.
3. Law enforcement can also work together by forming joint task forces and sharing resources.

Next to these three strategies, law enforcement agencies can also introduce new laws to battle the socio-economic impact on society caused by underground markets that facilitate cybercrime.

Table [x] provides an overview of actors, their interest level and possible strategies.

Table [x]: overview of actors, their interest level and possible strategies.

Actor	**Interest**	**Possible strategy**
Users of the platforms	Low	Stop using the underground markets.
Users of IoT devices	Low	Securing their own devices.
Internet Service Providers	Medium	1. Increase customer awareness for the need for secure practices. 2. Offering security software for free with subscription. 3. Offering free filtering of email with subscription. 4. Pressure other ISPs to take action. 5. Communication between ISPs and other parties on cases of abuse. 6. Not allow users onto the TOR network.
Security vendors	Low	Increase the security defences of their products.
Law enforcement from other countries	High	1. Share information regarding the physical location of a server which hosts a black market. 2. Share information regarding 'big fish'. 3. Forme joint task forces and sharing resources. 4. Introduce new laws and regulations.

6. Comparing risk strategies

In section 4 different strategies for the FBI's Cyber Division are described and section 5 describes possible strategies of other actors. In this section we will compare these risk strategies and discuss changes in risk strategies over time.

The actors have different strategies, mainly because they have different resources. Users of IoT devices can secure their own devices, but for example an ISP can not do this for them. The same goes for the possible strategies for ISPs, they can offer security software for free with subscription, but users of IoT devices or users of the platforms cannot do this.

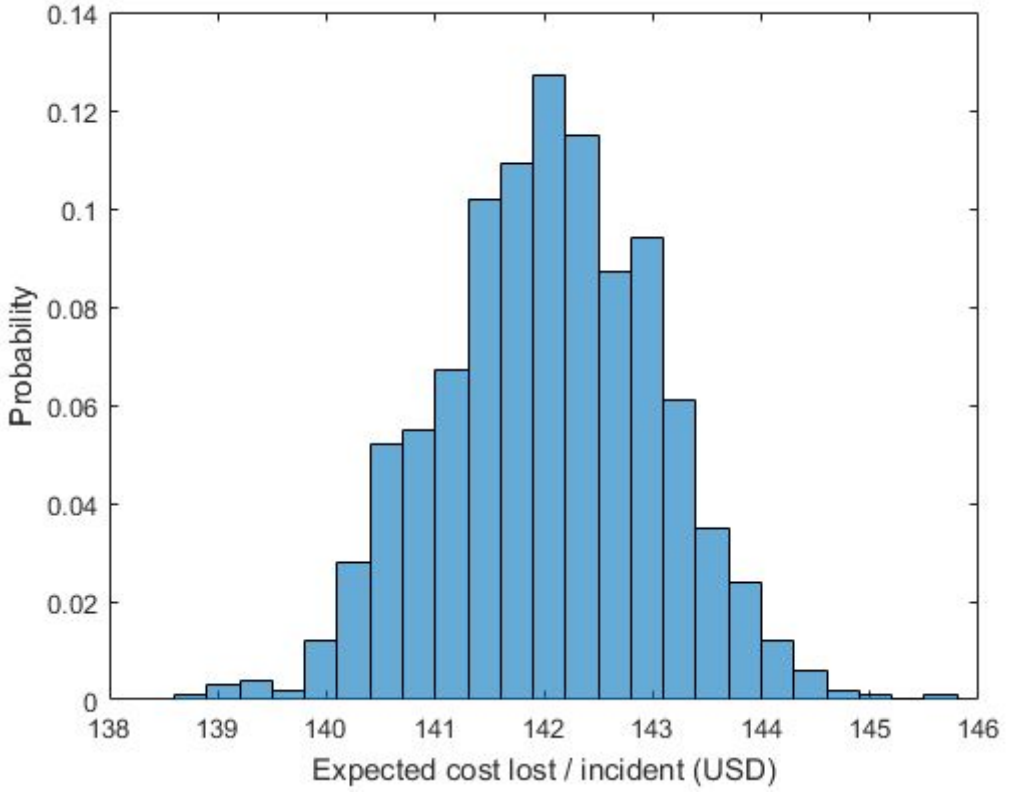
Over time, possible strategies for actors have changed. This can be because their resources changed or because their incentives changed. For example the incentives of ISPs have changed over the years (Van Eeten & Bauer, 2009). When the spread of viruses increased rapidly in the second part of the 1990s and an extensive amount of end users were infected, the main opinion of ISPs was that virus protection was the responsibility of the end users. Around 2001, when broadband connection and always-on connection grew, their opinion started to change. ISPs noticed their infrastructure could not handle all the traffic generated by the exponential increase of viruses and worms and needed to invest in network expansion if they decided to not reduce the impact of these viruses and worms. Because this would cost a lot of money, the ISPs incentives changed and they decided to act and fight against viruses and malware.

7. Return on Security Investment

The return on security investment (ROSI) can be calculated for our data set by calculating each component of it. There are 3 components: annualized loss expectancy (ALE), mitigation ratio and the expected cost of the solution. These three components will be described in the following sections.

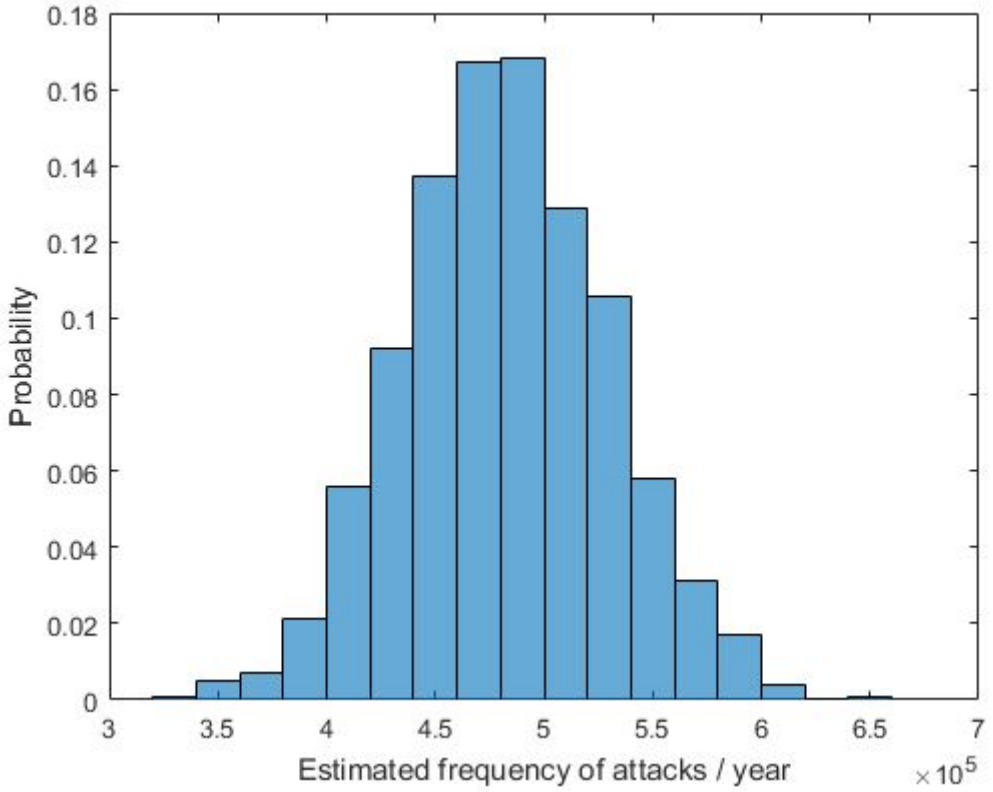
Annualized loss expectancy (ALE)

The ALE consists of 2 components: expected loss per incident * annual rate of occurrence. The first component is also called the single loss expectancy (SLE). This indicates the expected loss per incident in USD. This cannot be just a single number, they are discrete values. For this we assumed $142 as the expected loss from a single accident by Norton (2017) as the mean and .7% from the mean as the standard deviation for a normal distribution. We then made a probability distribution by using a monte carlo simulation. The result can be seen below in figure [X].

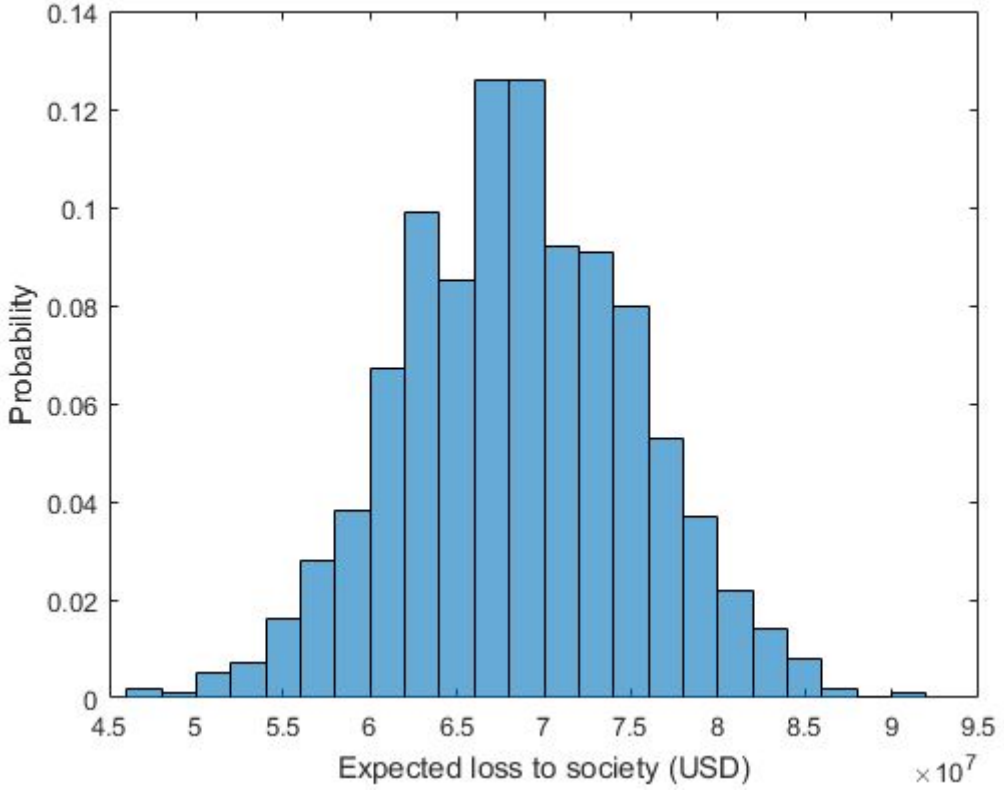


The second component is the annual rate of occurrence (ARO), this is the estimated frequency of attacks that occur within a year. We estimated this by looking at the total amount of transactions in the data set and subtracted the non cybercrime transactions from it, which results in 480.123 transactions. And from this we made an assumption that about 10% of the transactions are scam transactions, which do not have an impact on the society.

With this information we made another monte carlo simulation with a standard deviation of 10%, see figure[X].



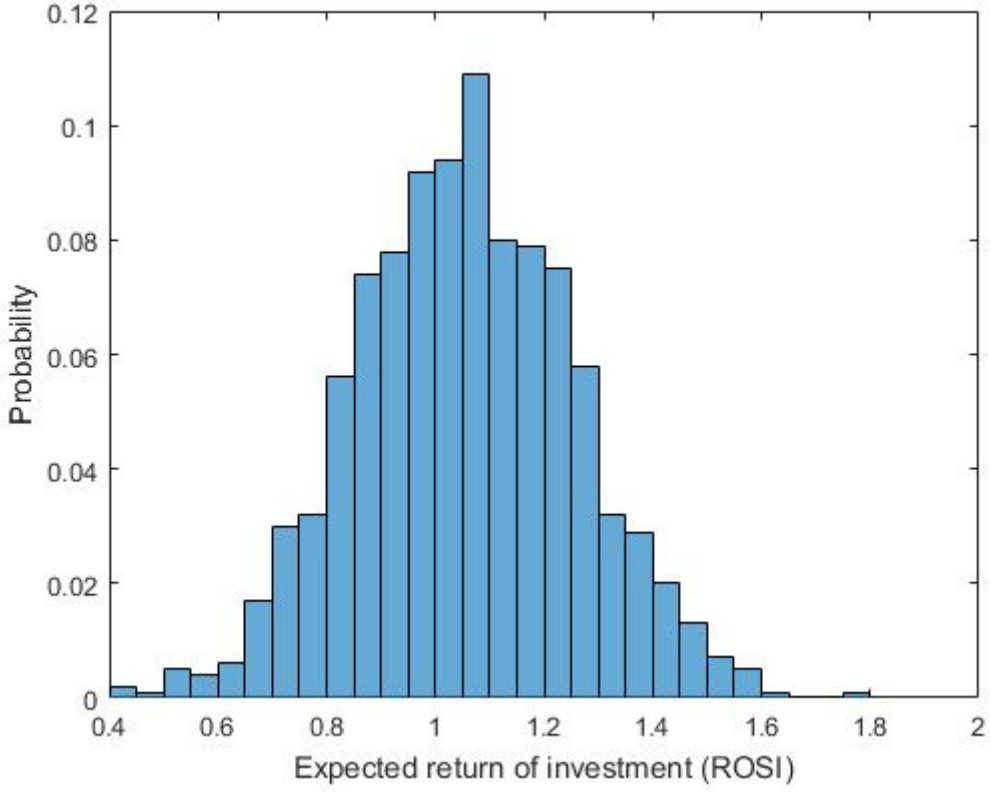
The ALE is the product of SLE and ARO. The estimated numbers can be multiplied in order to get estimated values for the ALE, see figure [X].



This graph describes the probabilities for expected losses to society per year. You can see that the expected loss is most likely between 60 million USD and 75 million USD. With this new information we can look into the cost of a solution and compare that to the expected loss.

Strategy Costs

For draft pruposes we chose a mitigation ratio of 30% with investment costs of 10 million.


0.12
0.1
0.08
0.06
0.04
0.02
0
Probability
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2
Expected return of investment (ROSI)

8. Conclusion

<Will be added in final version>

References

Europol. (2019, May 3). Double blow to dark web marketplaces [Press release]. Retrieved September 26, 2019, from https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

Kevin J. Soo Hoo. How Much Is Enough? A Risk-Management Approach to Computer Security. PhD thesis, Stanford University, June 2000.

Norton. (2017). Norton Cyber Security Insights Report 2017 Global Results. Retrieved September 26, 2019 from https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

Van Eeten, M & Bauer, J.M. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. Journal of Contingencies and Crisis Management 17 (4), pp. 221-232.