Underground Markets: Security and Risk Management - Block 3

WM0824TU Economics of Cyber Security - Group 16
October 7, 2019

EUR/USD - 1,35379 - 00:00:00 14 giu (EEST)
EUR/USD (Bid), Ticks, # 300 / 300
Gold, spot - 1,276,820 - 23:00:00 13 giu (CEST)
Gold, spot (Bid), 1 minute, # 159 / 300, Logarithmic, Heikin Ashi
Alerts
Settings
Quote List [2]
World Markets

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

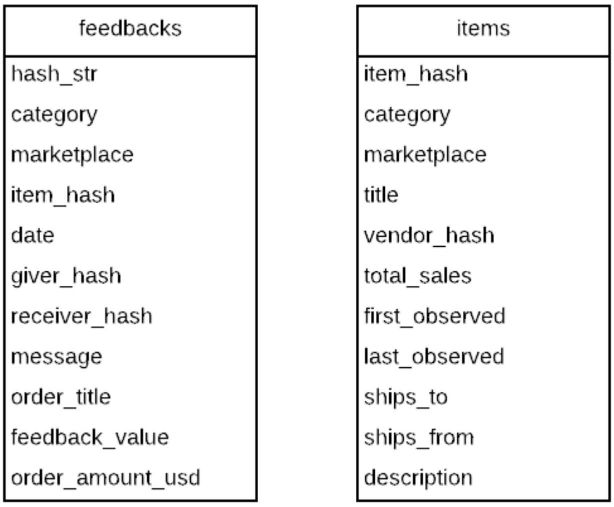
Table of Contents

1. Introduction

During the lectures we have learned the importance of measuring cyber security and the difficulties to determine the right metric. Security metrics are used to illustrate how security activities affect security goals and help make the right security decisions. This report examines data on underground markets from the data set *16_underground_markets* and develops security metrics and risk strategies to deal with the security threats posed by these markets.

Cybercrime has become highly professionalized and various “underground”, i.e., illegal, markets have risen. These supply various services required for a cyber attack (Franklin et al., 2007). This results in the phenomenon of cybercrime-as-a-service, making it possible to buy, for example, DDoS-services or fake credit card credentials in underground markets. In these markets there are sellers and buyers and moreover they are online, and hence can be defined as a multi-sided e-commerce platform (Asghari et al., 2016).

The data set on underground markets used for this project is a SQLite[1] database file, consisting of two tables, namely: `*feedback*` and `*items*`. Their decomposition can be seen in Figure 1.



feedbacks	items
hash_str	item_hash
category	category
marketplace	marketplace
item_hash	title
date	vendor_hash
giver_hash	total_sales
receiver_hash	first_observed
message	last_observed
order_title	ships_to
feedback_value	ships_from
order_amount_usd	description

Figure 1: Dataset decomposition

The item table consists of the listings offered and the feedback table consists of feedback given after a purchase including the receiver and giver hashes. Since these marketplaces usually require a mandatory feedback, the amount of feedback has been proven to be a good proxy for the minimum number of sales (Soska & Christin, 2015).

[1] https://www.sqlite.org/index.html

There also exist relations between the columns. For example, each feedback entry can be linked back to an items listing via the field `*item_hash*`. The relations also allow for the tracking of vendors across marketplaces (via the unique `*vendor_hash*` field).
These underground markets that facilitate cybercrime have a significant economic and social impact on society. An example is the ransomware WannaCry, which infected an enormous amount of computers all over the world and has a vast socio-economic impact (van Voorst, 2017).

In order to combat such issues, this report starts with identifying the problem owner in section 2. In section 3 the differences in security performance of the metrics of block 2 are discussed, after which risk strategies are identified in section 4. Section 5 identifies other actors relating to the security issue and possible strategies they can apply, which are compared in section 6. Finally, section 7 selects one of the strategies identified in section 4 and applies analysis in order to calculate a Return on Security Investment (ROSI) for applying the selected strategy.

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 mitigate this impact was identified as the law enforcement agencies (LEAs). In this report, we further narrow down this actor to a relevant 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 (FBI, n.d.). 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

The differences in security performance of the problem owner, the FBI CyD, can be evaluated by looking at the gaps in the total turnover per marketplace metric, visible in figure 2. The changes in the volume of transactions in the marketplace are sensitive to the actions of the law enforcement since the CyD (and other law enforcement agencies) target the markets that show the highest amount of activity to ensure their actions have the highest benefit.

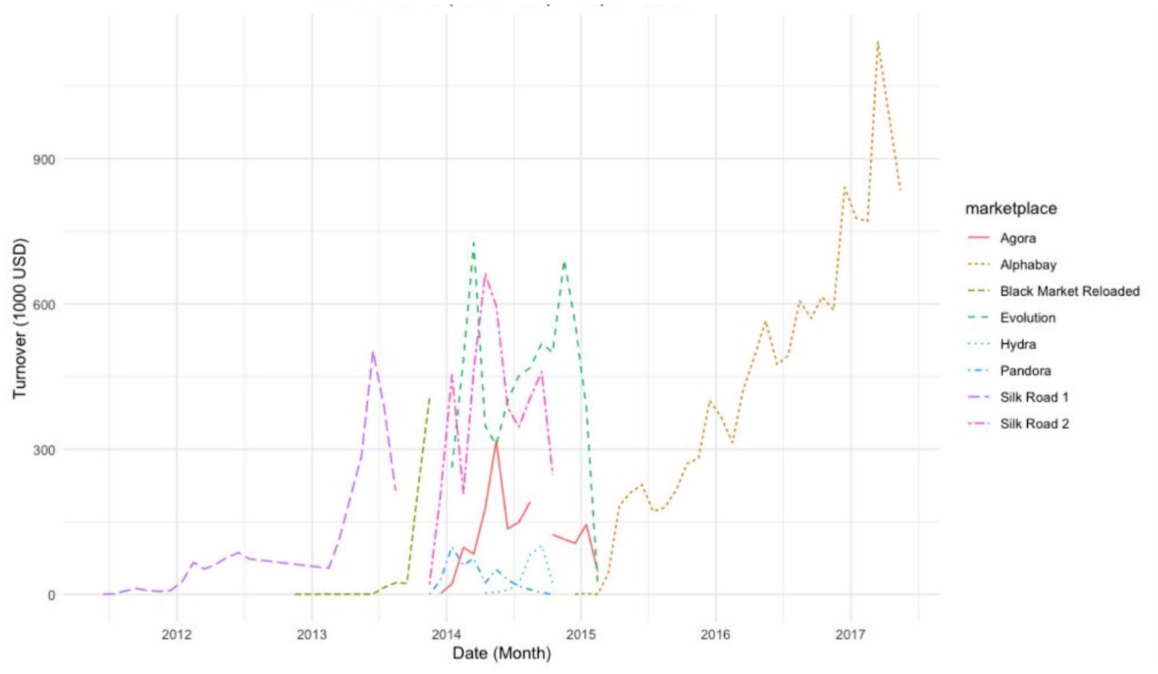


Figure 2: Total turnover per marketplace per month

In September 2013, ‘Silkroad 1’ was taken down by the FBI, the discontinuity in the graph in the latter half of 2013, reflects this action. Nonetheless, following the takedown of Silk Road, ‘Silk Road 2’ emerged after a gap of few months. In November 2014, Operation Onymous, a joint effort by the FBI and other law enforcement agencies took down ‘Silk Road 2’ and ‘Hydra’ (Soska & Christin, 2015). This can also be noticed in the graph: the data for Hydra and Silk Road 2 is only available between late 2013 and 2014. It is also interesting to note the spike in activity in Evolution following the take down of Silk Road 2 which could suggest migration of users of Silk Road 2 to Evolution.

In 2017, Alphabay was taken down by combined effort of the FBI CyD and other law enforcement agencies. This is reflected by the sharp drop in the graph for Alphabay in 2017. Along with Alphabay, two other marketplaces, Hansa and a Russian marketplace called RAMP (which are not available in our dataset), were also taken down. These three marketplaces accounted for almost 87% of all underground market activity (Interpol, 2018).

This metric thus reflects the actions of the FBI CyD and can be used to evaluate the effectiveness and performance of the FBI’s actions against the underground markets. We can see that in the years 2013 and 2014, the FBI participated in two effective take downs of underground markets with the next successful takedown occurring only in 2017. However, a simple comparison might be misleading since Alphabay was a larger market with higher volumes and turnovers and consequently the impact of the shutdown would be higher.

It is also important to note that marketplaces close and show differences in activity for a variety of reasons other than actions of law enforcement. In some cases, shutting down of marketplaces by the LEAs results in opening up of new marketplaces although their activity levels might be less. In other cases, the shut down of one marketplace causes other less prominent ones to shut shop too, due to security issues or because the owners abscond with the funds (Interpol, 2018). For instance, the marketplace ‘Agora’ stopped operations in August 2015 to address security issues owing to a vulnerability in TOR that allowed access to deanonymized server locations (Greenberg, 2015). As can be seen in figure 2, the shut down of Agora caused Alphabay to become the largest marketplace until it was taken down. Nonetheless, even with this caveat, when used within the context of evaluating CyD operations, it can serve as a useful measure for security performance.

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.

Currently, CyD organizes 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 the identification of threats related to national security activities and deterrence is the prevention of these threats through defensive countermeasures. Disruptions inhibits the threat actor's activities through actions such as arrests or the 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. These deterrence, detection, disruption, and dismantlement operations are part of CyD's existing mitigation strategy against cybercrime.

Efforts to target cybercrime originating from underground markets needs both technical expertise to conduct investigations on the darknet and expertise in the operational strategies to address the cybercrime. To this end, the CyD could choose to strategically increase its available pool of expertise in either areas and engage in skill building activities for its employees.

An increased collaboration amongst inter-governmental and international law enforcement agencies would enable increased knowledge and information sharing about the risks amongst these organizations and allow for coordinated activities against the underground markets.

To curtail the emergence and subsequent migration of activity to new marketplaces when existing ones are taken down, the CyD could adopt a dual focus of both taking down the individual marketplace while also prioritizing other high-level threats (eg. vendors and suppliers who trade large volumes) within the marketplace. This could prevent the movement of these threats to other marketplaces and thus make the intervention more effective.

In addition to that, special task forces can be setup to address particular cybercrimes that originate in the underground markets. For instance, a drug related task force could focus only on the drug related activities that occur across all marketplaces and thus develop a better picture of the overall drug activity in these markets. Following this information gathering stage, specialized niche strategies can be developed to only target the drug related activities and their impact. This would be useful since it enables expertise at the operational level of the cybercrime under consideration that the corresponding operational strategies to deal with drug related crimes would be different from other crimes like identity theft.

Further, 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. More specifically, using the information from previous attacks, for instance the type of malware against critical information infrastructure or information systems, further attacks against possible targets can be prevented. This would allow for a reduction in the security gap by creating a barrier against known attacks (Munk, 2015).

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. For instance, the CyD could handover the information about the risk to another agency e.g. Interpol, that might be better positioned to address and mitigate the risk. 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 cyber security policy.

Risk avoidance

Risk avoidance strategies typically involve withdrawing from the activity that incurs risk. However, since the existence of underground markets serves as an attractive platform for cybercrime, the risks here are the risk from all the categories of cybercrime that originate in these markets. And, since the CyD has the responsibility of combating cybercrime, the risk of which is spread over society as a whole, it cannot avoid the risk. Even measures such as banning TOR, even if technically feasible and within the scope of CyD's operations, would not be effective since it would lead to clever alternatives being designed for the crime activity. Additionally, with TOR being funded by the US government (Levine, 2014), the CyD may not have the incentive to do so even if it were feasible.

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 some, but not all possible risk 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 as 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 limited risk due to the absence of the need for direct interaction or coordination between buyer and seller (Van Wegberg et al., 2018). 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.

The users of the platform have multiple risk strategies. They can mitigate the risk by buying products with less impact on society or using what they bought in a different way, next to mitigation the users of the platform can also avoid the risk by stopping to buy the products sold on the underground markets. For the entire security issue to be avoided all users will have to quit, which has a low likelihood to occur.

5.2 Users of IT devices

The users of IT devices are the owners of those devices and thus have influence regarding the security of their devices. Users of IT devices are for example individual users or companies. The users of IT devices are victims and could be affected by the products sold on the underground markets. They can mitigate the security issue by 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. Even with mitigation, there always remains a residual risk. Users of IT devices need to determine their risk appetite and determine how much (residual) risk they want to accept. Accepting the risk can be done by accepting the residual risk or when they do not use any mitigation strategies, they can accept all risk. A third strategy the users of IT devices can apply is transferring the risk by the means of a cyber insurance. A cyber insurance is most suitable for risks that have a low chance to occur, but a high impact and will not be a fitting strategy for all users of IT devices.

Van Eeten & Bauer (2009) describe three reasons why users of IT 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 IT devices individually. The second reason is because users of IT devices might not be aware their machine is infected. Third, because many financial service providers offer compensation for losses incurred by their customers, this disincentivizes customers to be as secure as possible when dealing with their financial data. Because of these reasons, the users of IT 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.

In the role of victim the ISPs can choose to use a cyber insurance, for example insuring the damage that occurs when a DDoS attack is performed and there is too much traffic.

To understand the influence of the ISPs in the role of facilitators 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 and 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 reduce 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. This is a strategy to mitigate the risk.
2. Offering security software for free with subscription (Van Eeten & Bauer, 2009). This has the same mitigating 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 mitigating 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. Because the risk itself is not being transferred in this strategy, this is also a mitigation strategy.

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. This strategy can be categorized as both mitigation and avoidance. Because the existing black markets will be impacted, the strategy can be categorized as mitigation. But because this strategy also prevents new markets from arising, it is also risk avoidance.

5.4 Security Vendors

Security vendors can transfer their own risk using a cyber insurance. Next to that, they can mitigate the security issue by increasing the security defences of their products. 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 Software vendors

Software vendors can transfer their own risk using a cyber insurance. Software vendors can increase their competitive advantage by increasing the amount of users of their software. Because of this reason, software gets distributed quickly and updates are distributed later in time to remove security issues. A mitigating risk strategy the software vendors can take is therefore to wait a short period of time to distribute their software and to increase their security before distributing. Another mitigating risk strategy software vendors can take is to distribute security updates quicker, to do this they would need to invest more in finding and fixing the security issues. Because the first strategy would have a negative impact on their competitive advantage and the second strategy would require the companies to invest more, the software vendors interest to reduce socio-economic impact on society caused by underground markets that facilitate cybercrime is scored as low.

5.6 Market Owners

The market owners facilitate the existence of the underground market. Because this is illegal, they have an incentive to get the market offline. For the entire security issue to be avoided all market owners will have to take their market offline, which has a low likelihood to occur. Since the risk of being caught is low, this results in the market owners continuing to run the market and having low interest to reduce socio-economic impact on society caused by underground markets that facilitate cybercrime.

Table 1 provides an overview of actors, their interest level and possible strategies.

Table 1: Overview of actors, their interest level and possible strategies.

Actor	**Interest**	**Possible strategy**
Users of the platforms	Low	1. Stop to buy the products (avoidance) 2. Buying products with less impact on society (mitigation) 3. Using the bought products in a different way (mitigation)
Users of IT devices	Low	1. Securing their own devices (mitigation). 2. Accepting (part of) the risk (acceptance) 3. Use a cyber insurance (transfer)
Internet Service Providers	Medium	1. Use a cyber insurance (transfer) 2. Increase customer awareness for the need for secure practices (mitigation) 3. Offering security software for free with subscription (mitigation) 4. Offering free filtering of email with subscription (mitigation) 5. Pressure other ISPs to take action (mitigation) 6. Communication between ISPs and other parties on cases of abuse (mitigation) 7. Not allow users onto the TOR network (mitigation & avoidance)
Security vendors	Low	1. Use a cyber insurance (transfer) 2. Increase the security defences of their products (mitigation)
Software vendors	Low	1. Use a cyber insurance (transfer) 2. Increase software security before distributing new software (mitigation) 3. Distribute security updates quicker (mitigation)
Market owners	Low	Get the underground market offline (avoidance)

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 IT 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 IT devices or users of the platforms cannot do this. Multiple actors can transfer the risk, but only their own risk and not the risk for the society as a whole. Most strategies are directed to mitigate the risk.

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 mitigate the risk by fighting against viruses and malware instead of accepting the risk.

7. Return on Security Investment

In section 4 the different strategies for the problem are discussed. This section dissects the costs of the identified strategy of Risk Mitigation and evaluates the Return of Security Investments (ROSI) of said strategy.

Strategy Costs

The strategy chosen is that of Risk Mitigation as discussed in chapter 4. This strategy has been chosen since this is the strategy used in practice as discussed in the examples of chapter 3. Additionally, the alternative risk strategies do not result in any gain for the CyD. The costs of applying such a strategy can be split up into two types, namely direct and indirect costs. Direct costs are made out of the recurrent costs including expenses such as staff, equipment and software, etc. The indirect costs include costs such as variable costs and opportunity costs.

The direct costs are estimated using the FBI budget requests for 2020 (Wray, 2019) in which an additional budget of $70.5 million is requested solely for enhancing cyber investigative capabilities. Even though this value can be considered conservative, since it most likely does not cover the entirety of the cyber security budget of the FBI, the usage of the entire budget must also be taken into consideration. Since it can be assumed that the entirety of the FBI's budget of cyber security does not get invested into the take down of underground markets, we argue that this value can be considered as a valid estimate for the direct costs of taking down an underground market.

The indirect costs of the CyD can be assumed to be quite trivial. An example is opportunity costs, which is the difference in return, between the possible strategies. In this case, the other strategies do not return any benefits, therefore we do not take opportunity costs into account. We do have other indirect costs such as when the FBI encounter problems accessing data, hence they have a loss of productivity and need to develop tools to gain access. This budget is $38.3 million by FBI (2017). There are also possibly other indirect costs, but for simplicity we decided to not go into the details of other possible indirect costs.

Return on Security Investment

Using the estimated values, the return on security investment (ROSI) can be calculated for our data set. The ROSI consists of three components: the annualized loss expectancy (ALE), the mitigation ratio and the expected cost of the solution. The formula is as follows:

$$ROSI = \frac{(ALE * mitigation\ ratio) - solution\ cost}{solution\ cost}$$

Next we will go over each of these components.

Annualized loss expectancy (ALE)

The ALE consists of 2 components: annual rate of occurrence (ARO) * expected loss per incident.

The ARO is the estimated frequency of attacks that occur within a year. We can estimate this with the given data set, by looking at the total amount of transactions in the data set and subtract 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 can make an estimation by using monte carlo simulation with a standard deviation of 10%, see figure 3.

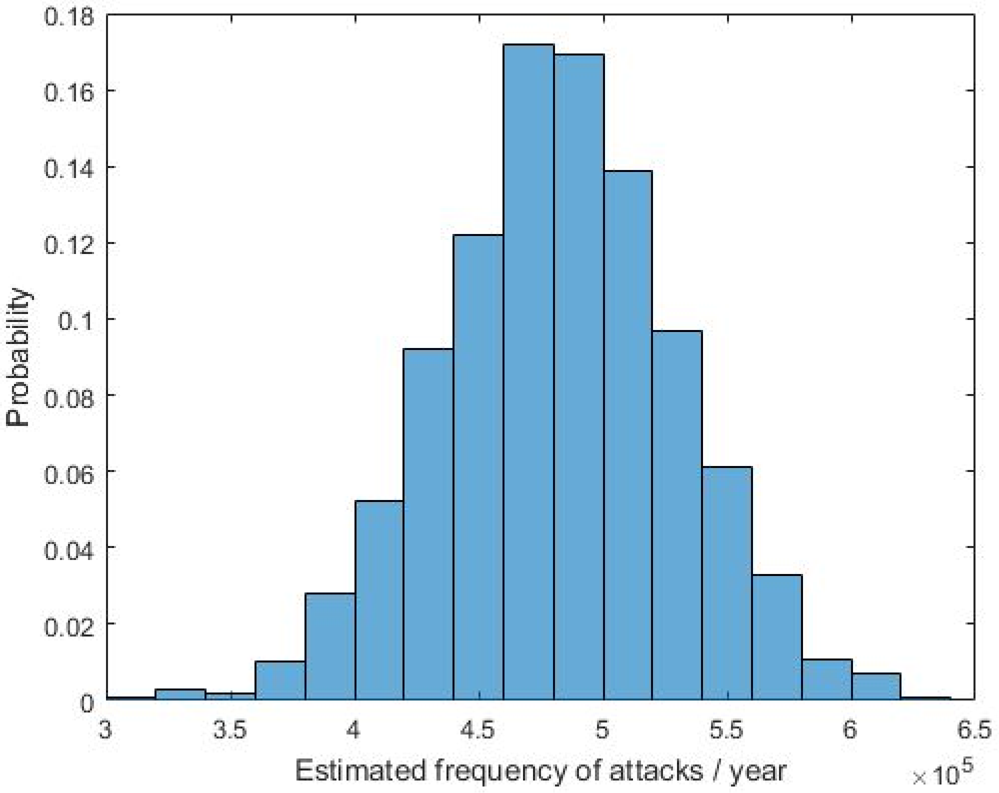


Figure 3: Expected annual rate of occurrence (ARO)

The second 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 4.

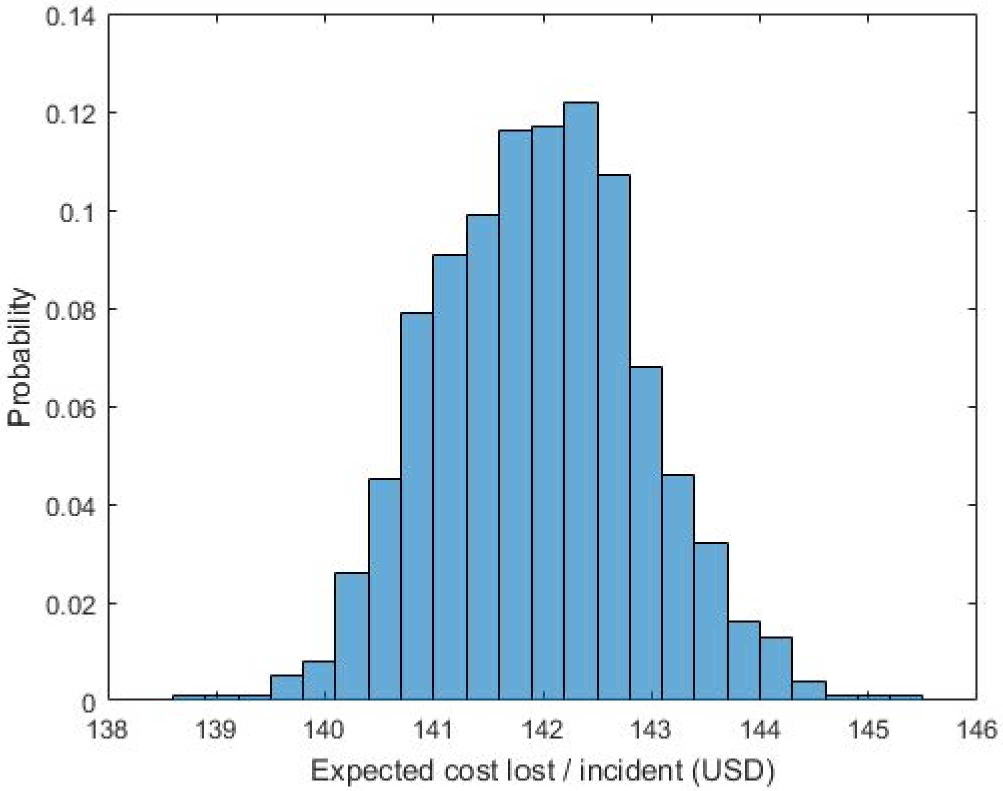


Figure 4: Expected loss per incident (SLE)

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 5.

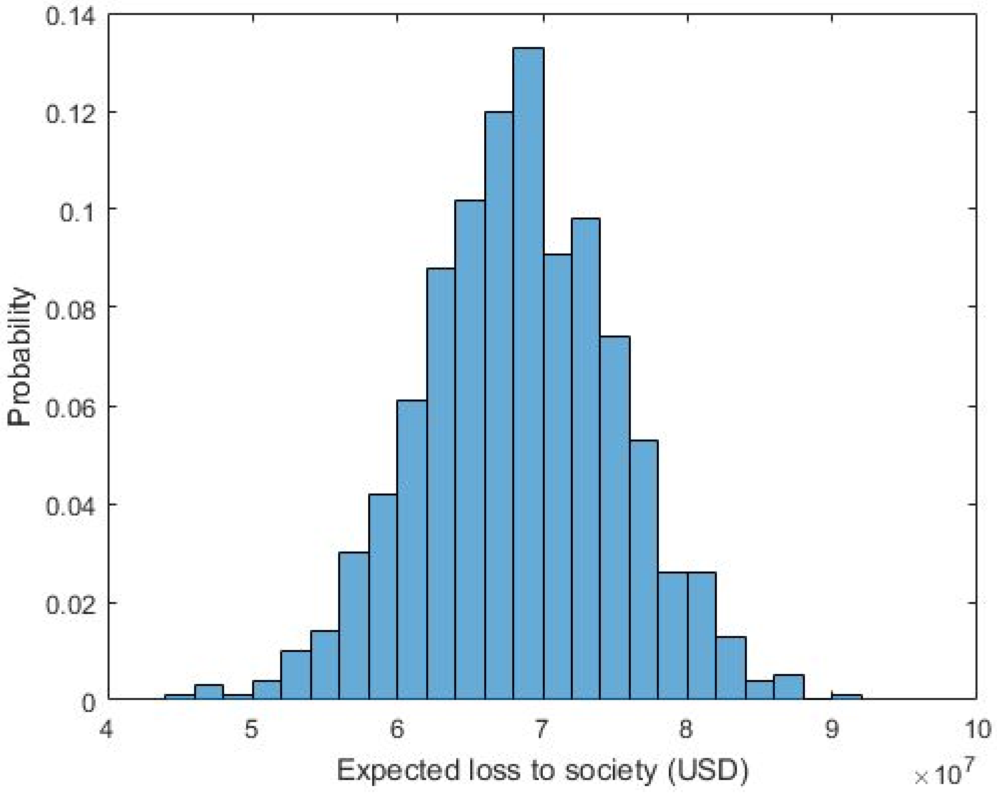


Figure 5: Annual Loss Expectancy (ALE)

Figure 5 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.

Calculation

For the ROSI, we use the combined costs of direct and indirect costs as the solution cost. This amounts to $70.5 million + $38.3 million = $108.8 million. We had chosen for a single number as estimation here instead of a range because it was difficult to find any information about the cost deviation. As for the mitigation ratio, we used 1 because when an underground market is taken down, we assumed that all losses caused by that market become 0.

The ALE was simulated by using a monte carlo simulation with 1000 trials. The ROSI is then calculated by using the results of each trial's ALE, with the mitigation ratio and solution cost as mentioned in this section. The ROSI can now be calculated by filling in all three components into the formula, in order to give a probabilistic ROSI distribution instead of a single number by calculating the ROSI 1000 times. The result can be seen below in figure 6.

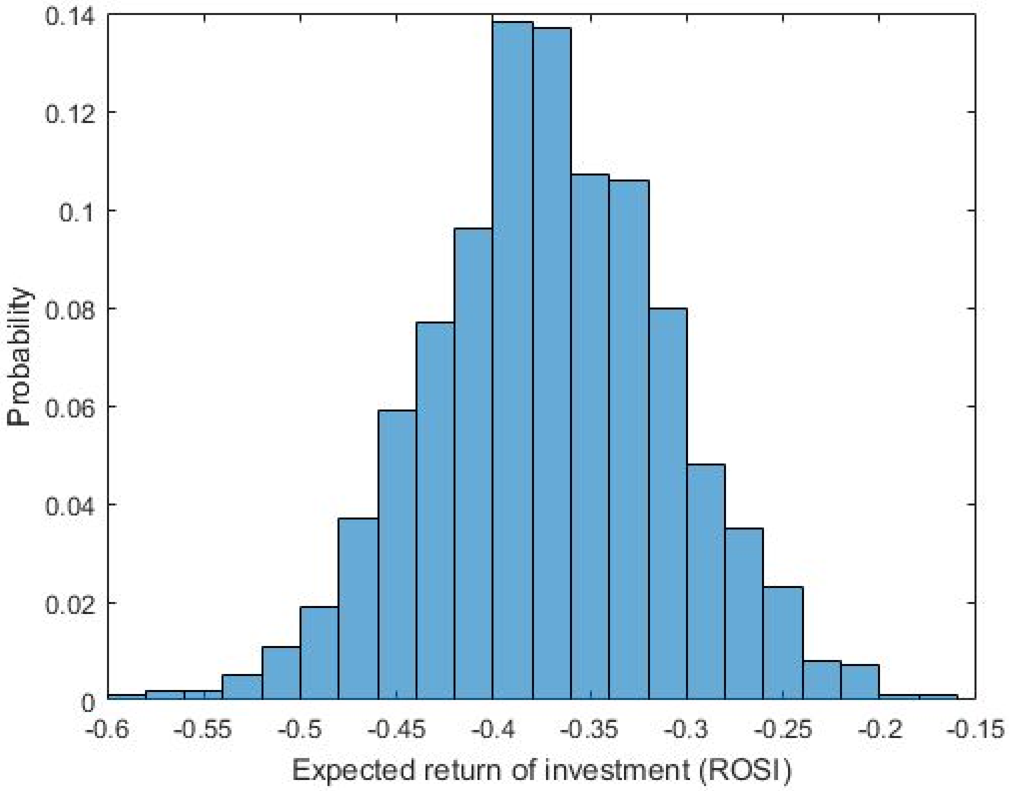


Figure 6: Expected Return of Security Investment (ROSI)

The ROSI appears to be negative, this is because the cost of solution is higher than the damages that are caused by the underground markets. For the problem owner, FBI's Cyber division (CyD) this is not necessarily an issue. As they do not directly carry any risk, they do not directly have anything to gain from this mitigation. However, this solution will take down an underground market and hence will decrease the identified security issue. This reduction will hence have a positive effect on the impact on society and therefore might have a positive ROSI in the long term.

Another factor that could be taken into account is that with respect to economic gain of such a take down. After the take-down of Silk Road 1 a grand total of 28.5 million USD in Bitcoin was seized by the FBI (Greenberg, 2013). Since every marketplace uses cryptocurrencies as their payment method, the taking down of other marketplaces could also result in such a seizure of said currencies, which could ultimately make the ROSI positive. This would then indeed indicate as to being a good investment. However, since it is not a given that this will be the case for all take-downs, this possible gain has not been taken into consideration for the calculations.

8. Conclusion

To conclude, we identified the problem owner behind the security issue, as defined in block 2, “*The socio-economic impact on society caused by underground markets that facilitate cybercrime”*. The identified problem owner is specified as the FBI’s Cyber Division (CyD). Next we illustrated that the metric total turnover per marketplace can be used to indicate the security performance. However it is not always reliable, since a shutdown of a market place could also result in the opening for another market place. Nevertheless, the metric can be used in the context of evaluating CyD operations. We identified the possible risk strategies the problem owner could follow. These strategies are: Acceptance, Transfer, Mitigation, and Avoidance. We also identified other actors possible of mitigation the security issue, these being: users of the platforms, users of IT devices, ISPs, security vendors, software vendors, and market owners. For each of these actors multiple possible strategies were identified. However, it became apparent that these actors do not have a high interest in performing these. Finally, the strategy of Risk Mitigation for the problem owner was selected as the most probable one. The costs of this implementing this strategy were dissected and a Return on Security Investment was simulated using the Monte Carlo method. The ROSI turned out to be a negative value, however this is not necessarily an issue for the product owner, because they do not carry the risk themselves. The solution will still have a positive effect on society and might result into a positive ROSI on long term once the underground market is taken down.

References

Asghari, H., Van Eeten, M., & Bauer, J.M. (2016). *Economics of Cybersecurity.*

FBI (2017) FBI Budget Request For Fiscal Year 2017. October 6, 2019 from https://www.justice.gov/jmd/file/822286/download

FBI (n.d.) What we investigate. Retrieved on September 28, 2019 from https://www.fbi.gov/investigate/cyber

Franklin, J., Perrig, A., Paxson, V., and Savage, S. (2007). *An inquiry into the nature and causes of the wealth of internet miscreants*. Alexandria: VA, pp. 375–88.

Greenberg, A. (2013). *FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road*. Retrieved October 6, 2019, from https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

Greenberg, A. (2015). *"Agora, the Dark Web's Biggest Drug Market, Is Going Offline"*. Wired. Retrieved 6 October 2019, from https://www.wired.com/2015/08/agora-dark-webs-biggest-drug-market-going-offline/.

Interpol. (2018). *Internet Organized Crime Threat Assessment*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Levine, Y. (2014). *Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government*. Retrieved October 7, 2019, from https://pando.com/2014/07/16/tor-spooks/.

Munk, Tine. (2015) *Cyber-security in the European Region: Anticipatory Governance and Practices*.

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

Soo Hoo, K., (2000). *How Much Is Enough? A Risk-Management Approach to Computer Security*. PhD thesis, Stanford University.

Soska, K. & Christin, N. (2015) Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *24th USENIX Security Symposium*, 33–48.

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.

Van Voorst, S. (2017) *WannaCry-ransomware in 150 landen*. Retrieved on 22 September 2019 from https://tweakers.net/reviews/5419/wat-maakt-wannacry-anders-dan-andere-ransomware.html

Van Wegberg, R., Tajalizadehkhoob, S., Klievink, B., Soska, K., Akyazi, U., Gañán, C., Christin, N. & Van Eeten, M. (2018). *Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets*.

Wray, C. (2019) *FBI Budget Request For Fiscal Year 2020.* October 6, 2019 from https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2020