# Underground Markets: Security and Risk Management - Block 4

WM0824TU Economics of Cyber Security - Group 16
October 21, 2019



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

# Table of Contents

# 1. Introduction

In the previous report, we analyzed the actors that were involved in the security issue. We also discussed the possible security strategies that they could take: accepting the risk, risk mitigation, transferring the risk, and avoiding the risk. This report builds upon the actors that we defined before and will discuss these in two parts. The first part of the report will focus on three actors: The FBI cyber crime division (CyD), internet service providers (ISP) and software vendors and their involvement in the security issue. We will discuss the mitigation of the security issue for each actor and the cost and benefits of this measure. Furthermore, we will analyze whether or not these actors have any incentives to take the strategy. In addition, the role of externalities regarding the security issue will also be discussed.
The second part will focus on factors that cause variance in the performance of our selected metric. Data is gathered from these factors, in order to perform a statistical analysis to analyze the impact. After this analysis, we will conclude this report with our findings from these two parts and the essence that is gathered from the statistical analysis.

# 2. Actors involved in the security issue

In this section, we elaborate on one concrete countermeasure the FBI Cyber Crime division, the Internet Service Provider, and the Software Vendor can take to mitigate the socio-economic impact on society caused by underground markets that facilitate cybercrime. We discuss their incentives to act or not to act and the distribution of costs and benefits we end with a discussion on possible externalities that may arise.

## 2.1 FBI Cyber Crime division

A concrete strategy that the FBI Cyber Crime division (CyD) could employ to mitigate the socio-economic impact of the underground markets is increased collaboration with other local and international law enforcement agencies. This could entail sharing sensitive information from the CyD's private investigations on the underground markets with other agencies, joint action with other agencies against the threats, increasing awareness about lesser-known threats and sharing resources as required amongst the agencies. This would allow the different agencies to develop a mutual understanding of the risks in the underground market landscape.

The actors involved in this strategy are the CyD and other law enforcement agencies (LEAs). The cost of the strategy might be unevenly distributed owing to the initial set up costs for the initiator. If the CyD initiates the collaboration, it will incur the one-time operational costs of planning and coordination for creating the collaborative framework. However, the costs of maintaining the collaboration, for instance, the cost of creating a central repository of information accessible by all collaborating agencies could potentially be shared amongst the agencies.

Ideally, the distribution of benefits associated with this strategy would be more or less equitable since all the involved agencies would have similar benefits. These include:

- Increased impact and effectiveness of operations against underground markets owing to the availability of more information
- Increased access to resources that might not have been accessible without the collaboration
- Synchronization of efforts to create interventions of maximal impact
- Prevention of duplication of effort across the agencies

Despite the significant benefits to the strategy, the incentives for the actors to take this strategy is quite limited owing to the high initial costs of the setup and the additional work for the CyD. Also, the collaboration brings the burden of increased interactions amongst the agencies and would need to gather a certain amount of momentum before the benefits can be reaped by the agencies. Hence, there might be resistance towards such additional efforts when there are no immediately viable benefits. Further, the unwillingness to share the glory

of a successful operation against the underground marketplace might act as a disincentive towards the collaboration.

## 2.2 Internet Service Provider

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 cyber crime and they also facilitate the existence of these underground markets. One concrete countermeasure the ISPs could take to mitigate the socio-economic impact on society caused by underground markets that facilitate cybercrime is offering security software for free or a low price with a subscription.

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

The costs to maintain the security software is for the ISPs. They may decide to use a third party for this, who will reap some benefits. The ISP subscribers often do not know their device is infected, and therefore will not directly see any benefits. The ISPs themselves will reap some benefits as well, although by indirect effects. When more customers have installed good antivirus software, this will result in fewer security incidents and fewer customers contacting ISPs with questions related to security incidents. Installing good antivirus software will also lead to fewer possibilities for devices being used for for example DDoS attacks, thus resulting in less traffic on the network.

## 2.3 Software Vendors

Software vendors can increase their competitive advantage by increasing the number 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 distribute security updates quicker, to do this they would need to invest more in finding and fixing the security issues. Because this strategy would require the companies to invest more, the software vendors' interest to reduce the socio-economic impact on society caused by underground markets that facilitate cybercrime is scored as medium.

Software Vendors pay the costs and receive little benefits. The benefits they do get are in the sense of reputation building. Most other actors in this scenario are benefited by this

strategy. Because there are fewer vulnerabilities for attackers to exploit, fewer users of IT devices get infected by malware and the ISPs get the same benefits as described in the section above, without needing to invest.

## 2.4 Externalities

In this case, multiple externalities can be identified. A positive externality is a benefit to a third party that is the consequence of another's actions and a negative externality is any harm that is imposed on a third party as a consequence of another's actions.

On underground markets, cybercrime products are sold, resulting in turnover for the sellers and an investment for the buyers. Some of the products sold, for example, malware or botnets, can be used by the buyers to affect other people. The trading on these markets and the usage of products bought can have side effects or externalities. The first externality that occurs is due to the usage of products bought on the market. When these products are used, they may target just an individual system or a group of systems. However, they can also affect other systems, who were not initially targeted.

The second externality important to consider in this case is a network externality. This means that the larger the network is, the more valuable the product is to each of its members. In this case, the product is software sold by Software Vendors. For example, as more people use the software, more applications get developed for it, thus making the software more valuable. As was said in the section before, it explains why Software Vendors do not make their Software as secure as possible before distributing it, resulting in vulnerabilities in the software.

On the other hand, when Software Vendors do make their software more secure before distributing it, this will result in costs for them, but the most benefits are reaped by the users of the software since those systems are more secure, which also mitigates the socio-economic impact on society caused by underground markets that facilitate cybercrime.

The fourth externality is interdependent security. Since almost all systems are connected through the internet, they are dependent on each other for their security (Moore, 2010). This means that when systems you have a direct connection to, are secure, you yourself are more secure as well, even if your system is not protected as well as the other systems. This also goes the other way around. Even when your system is protected very well, your system is less secure if systems close to you are less secure. This can be related to the ISPs. ISPs create a positive externality by offering security software with a subscription by making multiple systems more secure at once, even the ones they do not offer free security. But because they are interdependent with systems connected by other ISPs, who might not be as secure as they are, this also negatively affects ‘their’ systems. Because of this reason ISPs might decide to not invest in security software that is free or costs little for the consumer.

# 3. Security Performance

The selected metric is visible in figure 1. This metric shows the number of vendors in the top 20% of the total vendors across all marketplaces per month. These are the vendors whose combined sales contribute to 20% of total sales. Showing only the top 20% of all vendors allows for tracking the total number of big vendors. Based on the fluctuations of this value, we can make assumptions on the effectiveness of the security performance of the previously identified actors. In addition, this metric excludes all listing of category “other” as these do not include any relevance to the topic of Cyber Security.

As discussed in Block 2, on September 2013, ‘Silkroad 1’ was taken down by the FBI, this discontinuity is reflected in the latter half of 2013 in the graph, where a drop is noticeable. 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: we can see an enormous decrease in the number of active sellers in the latter half of 2014. In 2017, Alphabay was taken down by the combined effort of the FBI CyD and other law enforcement agencies. This is reflected by the ending of data in the graph in 2017. Hence we can draw the conclusion that the security performance of the actor Law Enforcement Agencies (LEAs) is visible in the metric of figure 1. In our case, the identified actor is also the problem owner as explained in Block 2.

We can also note that the trend of the number of sellers was actually going up during the duration of the dataset, however, this does not necessarily mean that the LEAs did not achieve any relevant security performance since this could simply mean that an increasing amount of people are using black markets.

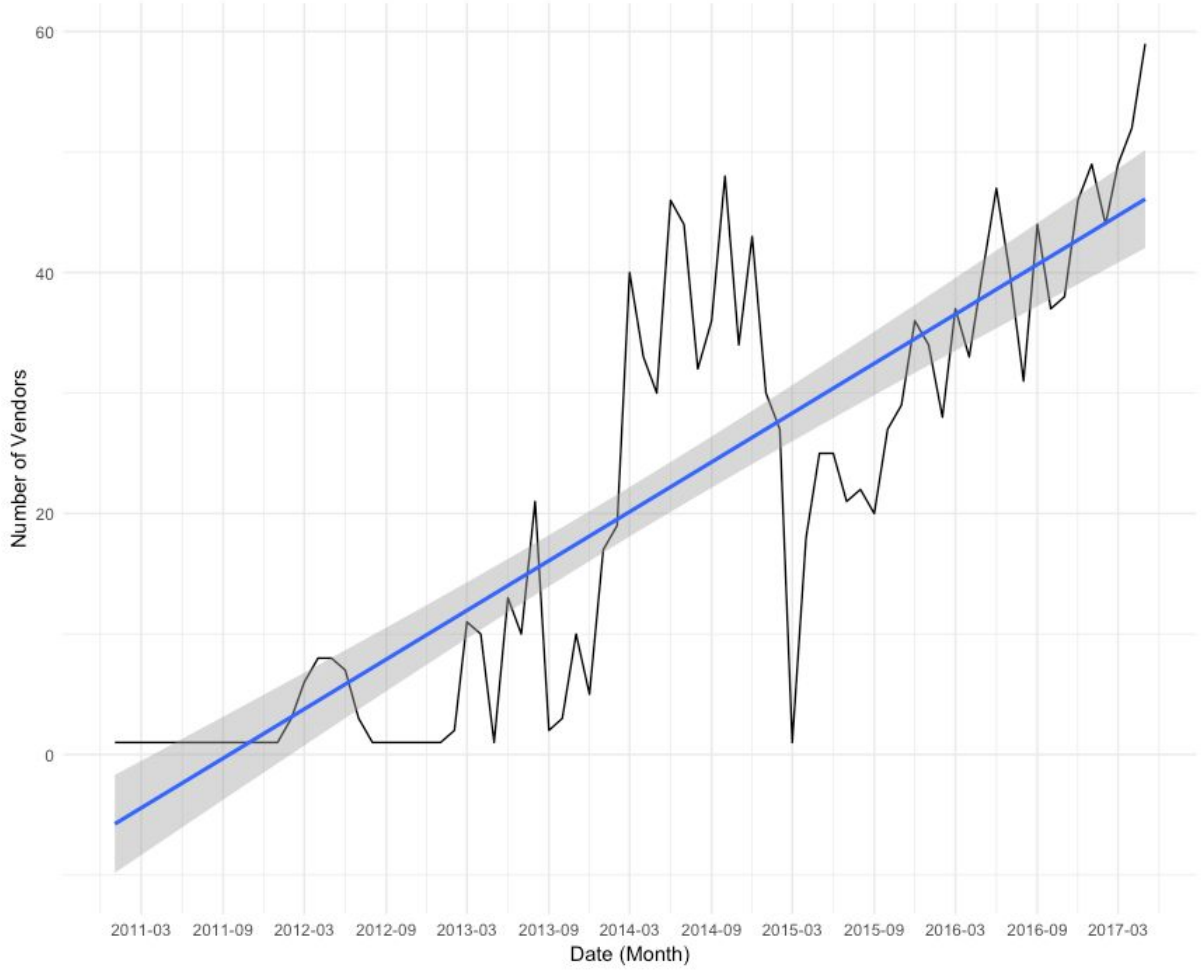


**Figure 1**: Amount of vendors in the 20% percent of vendors per month

## 3.1 Different factors of the metrics

One can notice a lot of variance in the data visible in figure 1. There are several factors that explain these (and thus influence) these variances. The first major factor is that of takedowns by the LEAs as discussed earlier in this section. The LEAs are responsible for the takedowns of “Silk Road 1”, “Silk Road 2”, “Hydra”, and “Alphabay”. After each takedown clear regressions are visible in the number of sellers. Hence the first factor is that of the number of active marketplaces.

A second factor capable of influencing the number of active sellers is that of the number of sales. In case the demand for cybercrime wares decreases, the supply will inadvertently also drop and subsequently, the number of vendors in case being one becomes less lucrative. This ties into LEAs when they arrest large vendors, takedown marketplaces or target buyers as was the case in Vleugels (2018). This can scare off potential buyers and subsequently lower the number of sales.

The third factor is related to countries. Certain countries have more active approaches to targeting underground markets. An example of this is the FBI CyD targeting (large) vendors

in the examples discussed in Block 2. In addition, this is visible in DarknetLive (n.d.), which holds a list of vendor arrests, with a quantity of 130 as of writing this paper. These examples might scare of potential or existing vendors, especially if it becomes apparent that a lot of vendors from their specific country are apprehended by LEAs. Hence we can assume that the country influences the number of vendors present.

## 3.2 Statistical Analysis

We performed statistical analysis to analyze the impact on the factors identified, “no. of active marketplaces”, “amount of sales” and “countries” on the metric of “active vendors across all marketplaces. Since the data we have does not follow a normal distribution, the Kendall correlation was calculated for each. To get more meaningful results, the average number of sellers per month was grouped into intervals of 10 (0-10, 10-20, …, 170-180) and the means of number active marketplaces, sales and country was calculated across the whole interval.

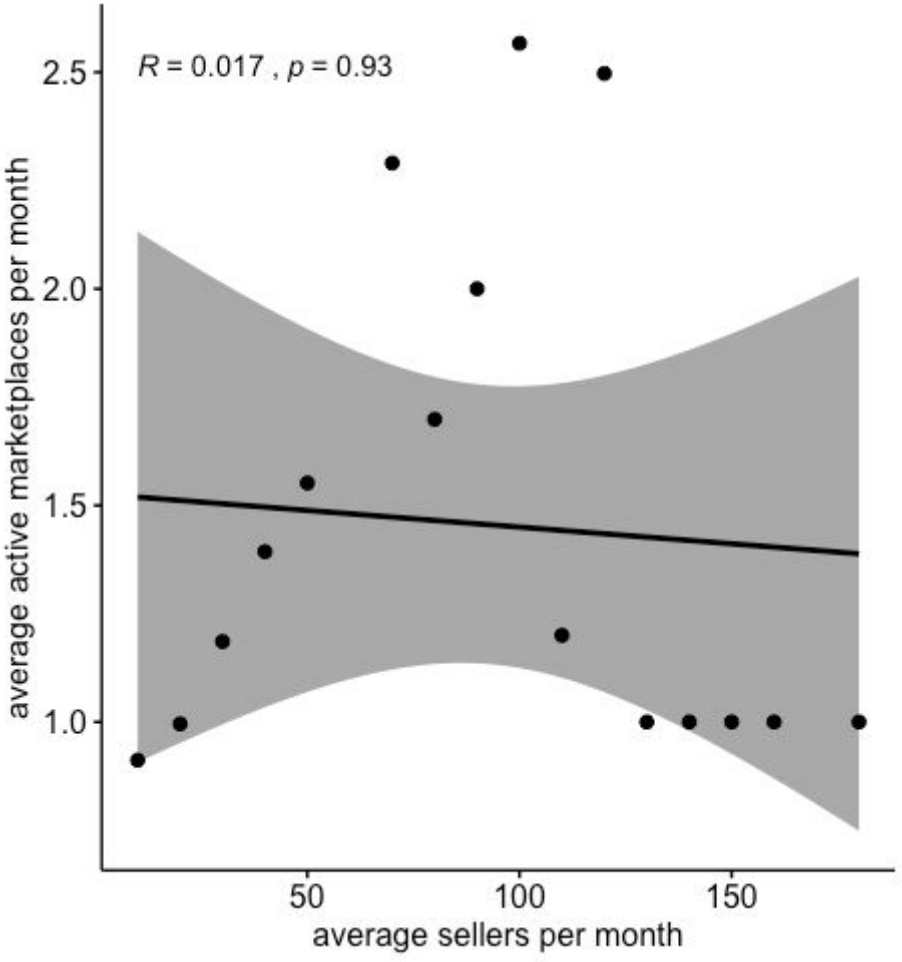


**Figure 2**: Correlation between average active marketplaces per month and the number of active sellers per month

From figure 2, we can observe that the number of sellers and the number of active marketplaces have a small correlation of 0.017 and a p-value of 0.93. Thus, there isn't any statistically significant relationship between the average number of sellers and the average number of active marketplaces per month for the data in our dataset. This could be because across the entire dataset there is very brief period between late 2013 and early 2015 where there were more than one marketplace open. For the rest of the time period, the number of sellers might relate to the popularity of the open marketplace, more popular marketplaces attract more sellers as is seen in the extreme right where we see high number of sellers even though only one marketplace is open.

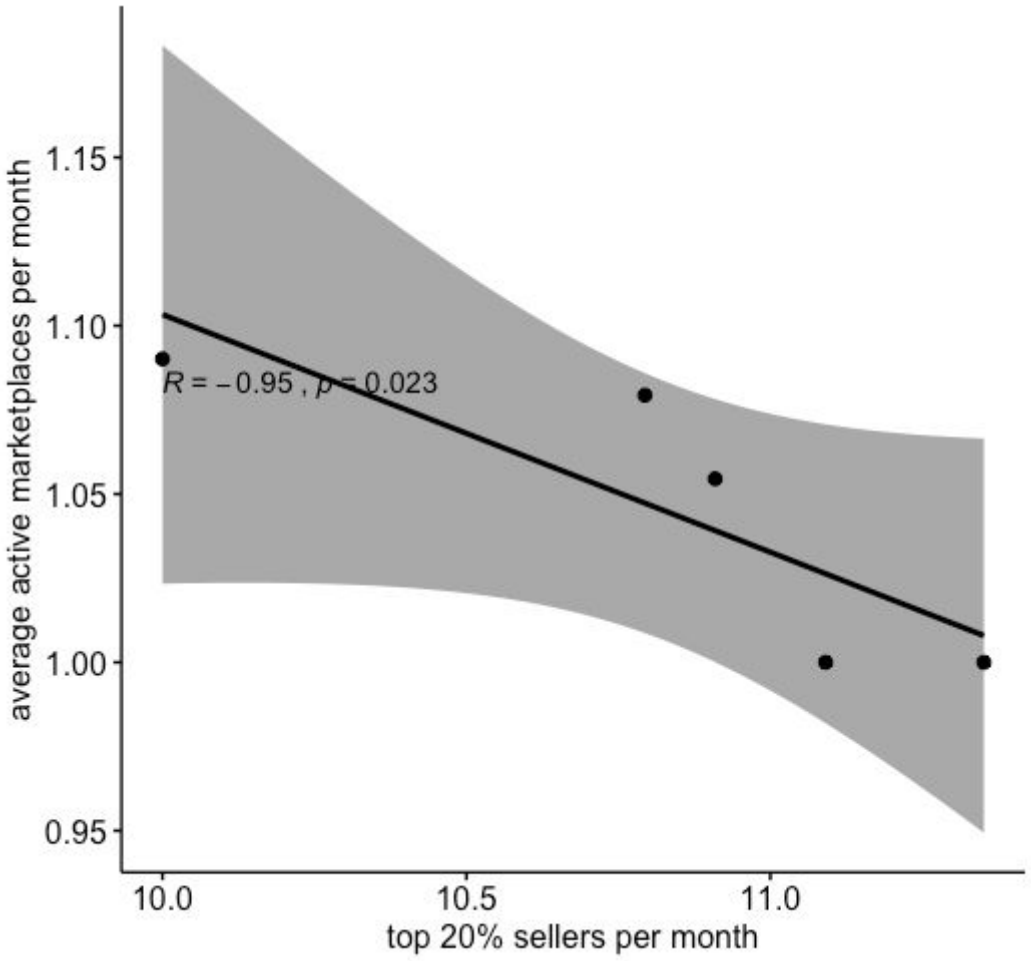


**Figure 3**: Correlation between average active marketplaces per month and the top 20% sellers per month

From figure 3, we can see the correlation between the top 20% of sellers and the active marketplaces. Although not statistically significant, it shows that the top sellers choose to operate and are active only in one marketplace.

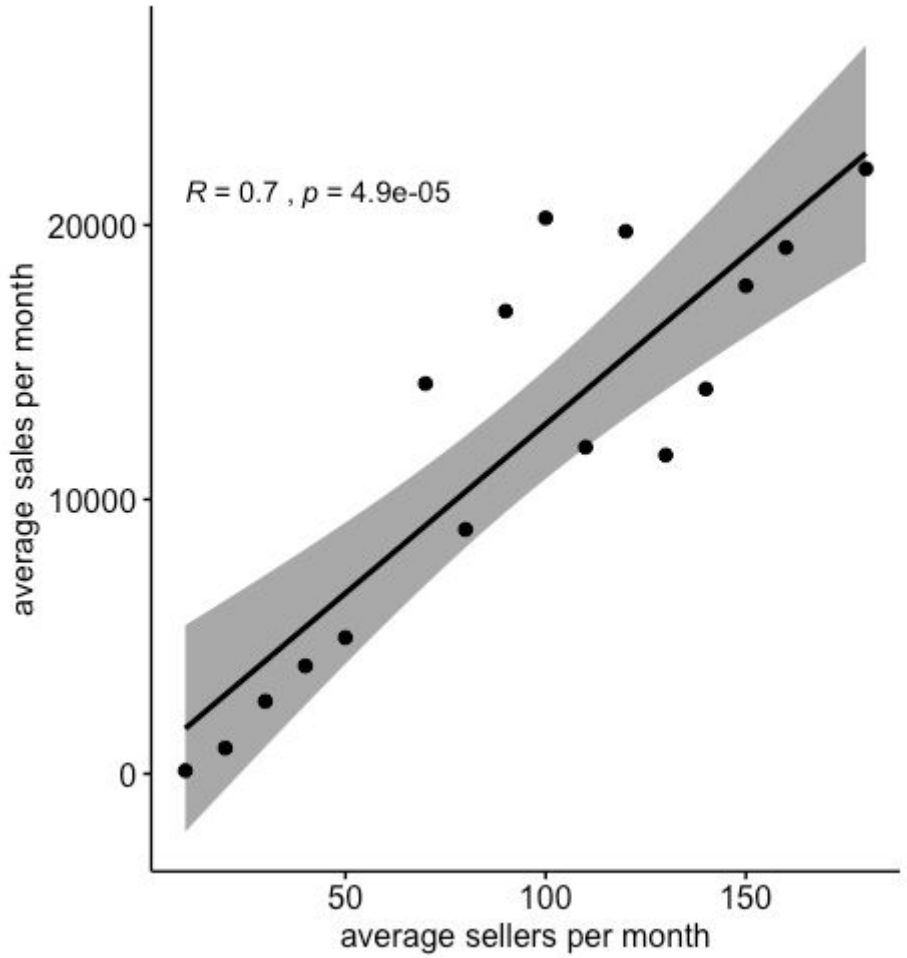


**Figure 4**: Correlation between average sales per month and the number of active sellers per month

From figure 4, we observe a high correlation of 0.7 between the number of active sellers in the market and the total amount of sales made on a given day. Though this is a statistically significant and an expected relation, it is interesting to note that the distribution is spread towards the middle and is not a perfectly linear relationship, a very high number of sellers does not always lead to a correspondingly high increase in the sales.

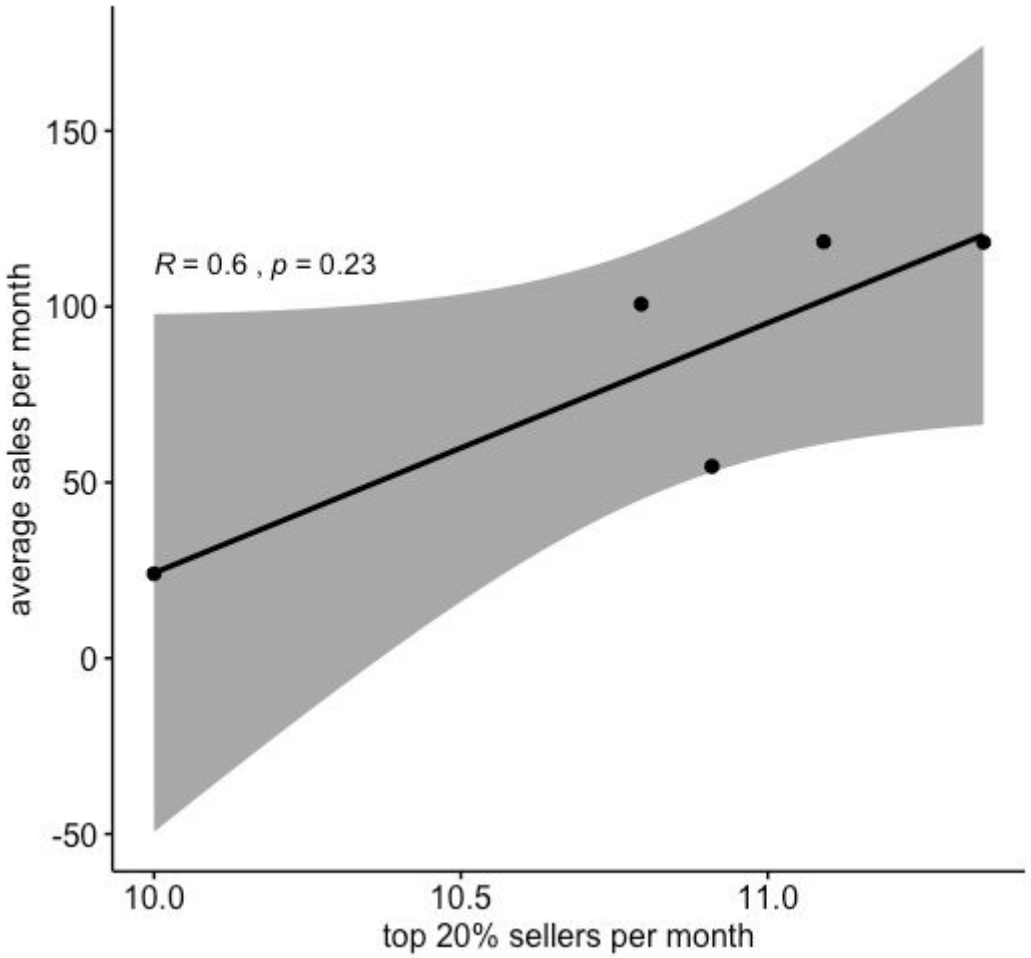


**Figure 5**: Correlation between average sales per month and the top 20% sellers per month

Figure 5 shows the correlation between the average sales of the top 20% of sellers per month and the number of sellers in the top 20% of sellers.

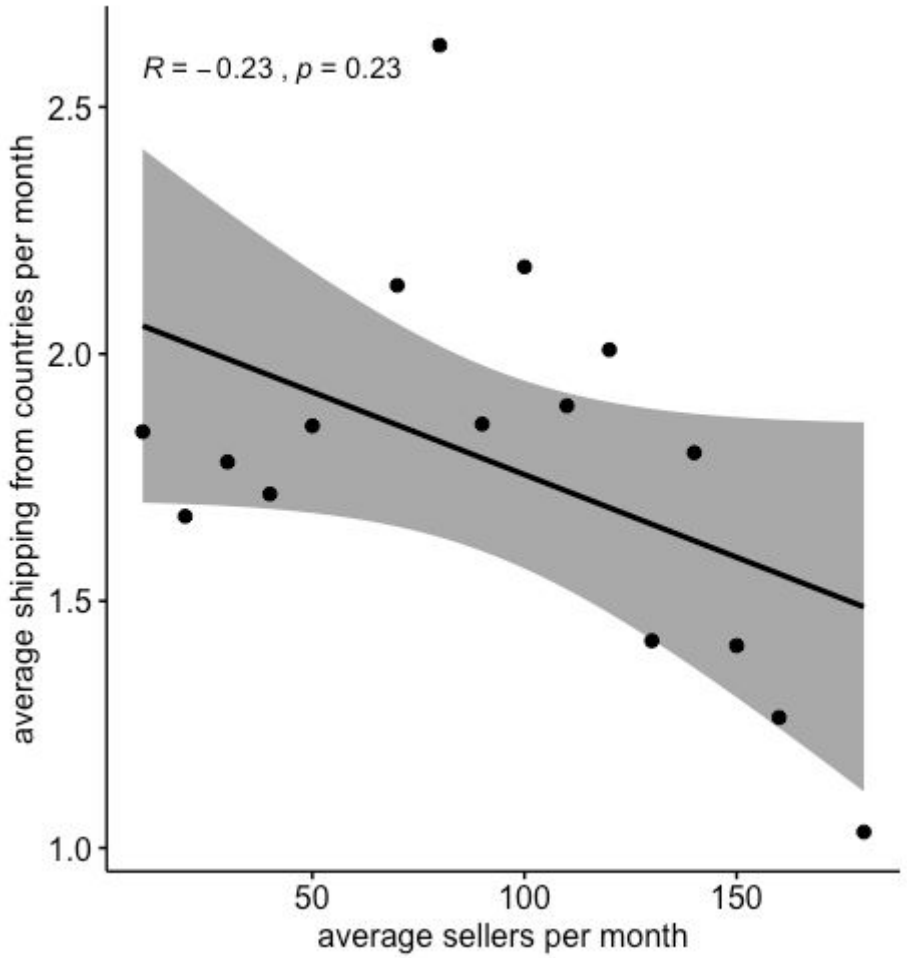


**Figure 6**: Correlation between the average number of seller countries per month and the number of active sellers

From figure 6, we can observe the relationship between the country of the seller, which is identified as the shipping from location and the total number of sellers. Interestingly, it exhibits a negative correlation of -0.23, but it is not statistically significant.

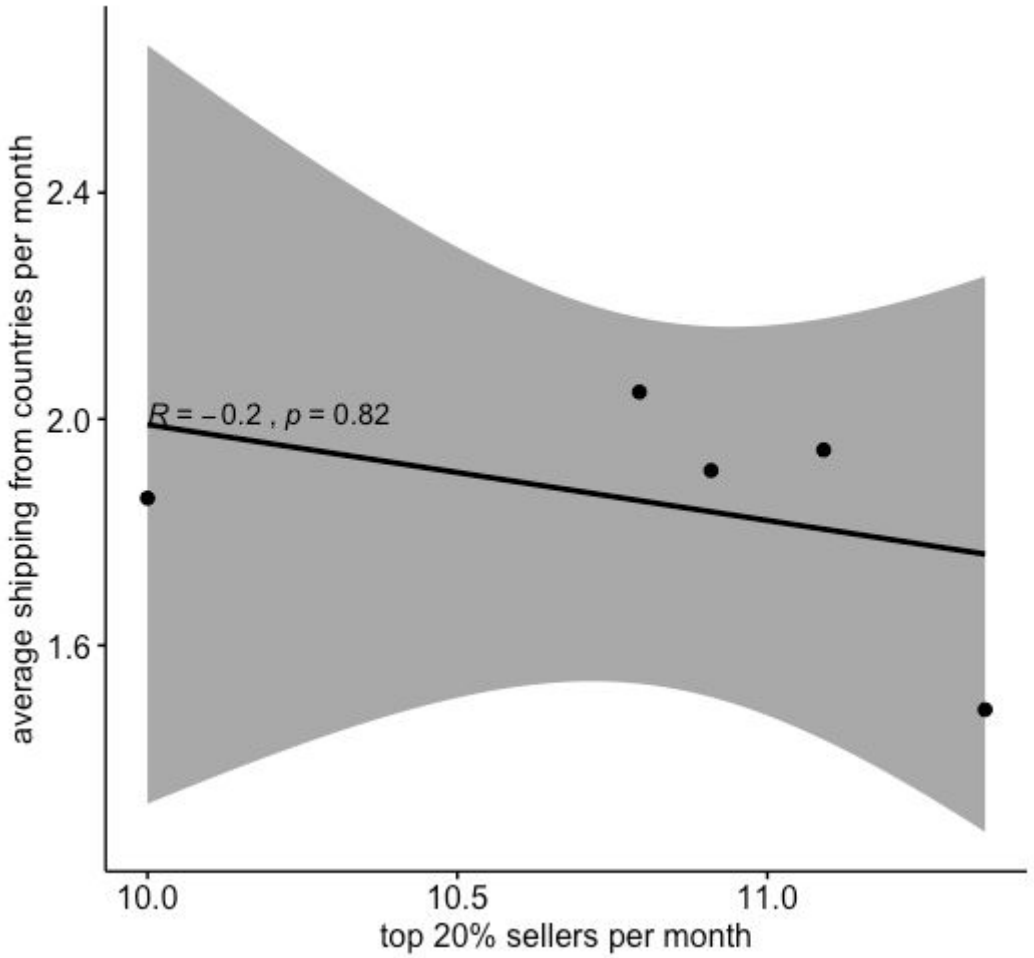


**Figure 7**: Correlation between the average number of seller countries per month and the top 20% sellers per month

From figure 7, the correlation between the average number of countries that the top 20% of sellers operate in and the top 20% of sellers can be observed. We can see a negative correlation of -0.2, indicating no statically significant correlation.

# 4. Conclusion

The first part of the report focussed on three actors: FBI cybercrime division (CyD), internet service provider (ISP) and software vendors and their involvement in the security issue. The CyD can increase its collaboration with other local and international law enforcement agencies to mitigate the security issue. This has the benefit that it allows a mutual understanding of risks in the underground markets and increasing the effectiveness of the takedown operations of underground markets. The incentive is limited due to the high initial costs of the setup and the additional work for the CyD.
The second actor mentioned is the ISP, they could mitigate the security issue by offering security software for free or at a low price with a subscription. It has the benefit of fewer security incidents which leads to fewer customer inquiries, this is an incentive to execute this measure. However, they also have disincentives which include legal risks, possible constraints and the cost of customer acquisition, hence their incentive is scored as medium.
The third actor mentioned is software vendors, they could mitigate the issue by distributing security updates rapidly. This strategy requires them to pay costs to receive small benefits themselves. Their incentive is scored as medium, as they do get a better reputation since fewer users of IT devices get infected by malware.
We also identified four externalities that are related to trading in underground markets and the usage of such products. The first externality is the products purchased from underground markets may also affect systems that were not initially targeted. The second externality is network externality that involved the software vendors, the more people use their software, the more valuable it becomes. The third externality is the users that reap the benefits of using more secure software which reduces the impact of the security issue on society. The final externality that we covered is interdependent security. One ISP could make multiple systems more secure, however, this might negatively affect systems of other ISPs that are not as secure.
In the last part of the report, we looked at three possible factors that caused variance in the security performance. The first factor is the takedown of underground markets by LEAs. We investigated this by looking at the average number of active market places per month with the average amount of sellers per month, which had no statistical significance. The second factor is the amount of sales from big vendors that might influence the number of active sellers. This gave a high correlation as expected, however a very high number of sellers does not always lead to a correspondingly high increase in sales. The last factor was related to countries that are more active in targeting underground markets. We analyzed the average shipping from countries per month with the average sellers per month. The result gave a negative correlation, however it was not statistically significant and could be a coincidence.

# References

DarknetLive. (n.d.). Arrested Darknet Vendors. Retrieved October 14, 2019, from https://darknetlive.com/arrested-darknet-vendors/.

Moore, T. (2010)., Introducing the Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection.*

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.

Vleugels, A. (2018). *This is how Dutch police know you're buying drugs online*. Retrieved October 14, 2019, from https://thenextweb.com/the-next-police/2018/08/07/police-drugs-online-darkweb/