# Cybercriminal Markets

Economics of Cyber Security Assignment Block 3

Erin Bartholomew, Marrit Hoppenreijs, Christian van Bruggen, Sarah Vetter

Delft University of Technology

**Abstract:** Cybercriminal markets host a large number of sales of illegal goods, both physical and digital. The challenge of tracking and stopping those sales falls on several national and international organizations. In the Netherlands, the Dutch National Police maintains significant responsibility for reducing cybercriminal activities on these underground markets. By analysing the costs and benefits of a proposed risk management strategy, the Return on Security Investment (ROSI) can be determined.

**Keywords:** cybercriminal markets, underground forums, ROSI, risk strategies

## 1 Introduction

As analyzed in the previous paper, security in cyberspace has a value, which differs depending on the perspective of the decision maker. Per Ghernouti-Hélie [1], the purpose of cybersecurity is to deliver a contribution towards the preservice of contingents and resources of a nation to meet its goals. Those include the safety and sovereignty of the state, security of critical infrastructures, public safety, security of human lives, and economical security.

This paper identifies different actors and their risk strategies pertaining cybercriminal markets and analyzes the costs and benefits of a proposed risk strategy in order to determine its Return on Security Investment (ROSI)..

## 2 Problem owner

The authors of this paper identified that in regards of the Netherlands, the security issue of cybercriminal underground markets is the trade in illegal products, both physical and digital such as drugs and malware, that might be result in violence and damage the Dutch citizens' well-being. The problem owner of the security issue is the Dutch national police, who conducts security operations in order to protect the national security of the Dutch citizens. For this reason, the police operate from the perspective of the "defender" side to defend the national security, thus not the security of one organization.

## 3 Current security performance

The primary security metric category developed to analyse success of the Dutch High Tech Crime team is the number of and total sales originating in the Netherlands and other countries over the time period represented in the dataset. There are two limitations to note from this metric. First, that this represents the number of sales postings that originate in The Netherlands, and not actual sales made. Second, that data measured does not represent number of units per sale, but either number of sales and total sales cost.

First, the number of sales per month and total sales per month are plotted for each forum and each country separately. These are found in Figures 1, 2, and 3 on the following page. The similar peaks and valleys in these graphs reveal common sales posting activity in each country over time.

Second, by examining the total sales per month as opposed to instances of sales postings, the forums that likely move the largest quantity of product are made more clear. In this case, it becomes clear that for each country, Silk Road 1 and Silk Road 2 both had higher quantities of sales at their peaks than other forums.

# Number of Sales per Month

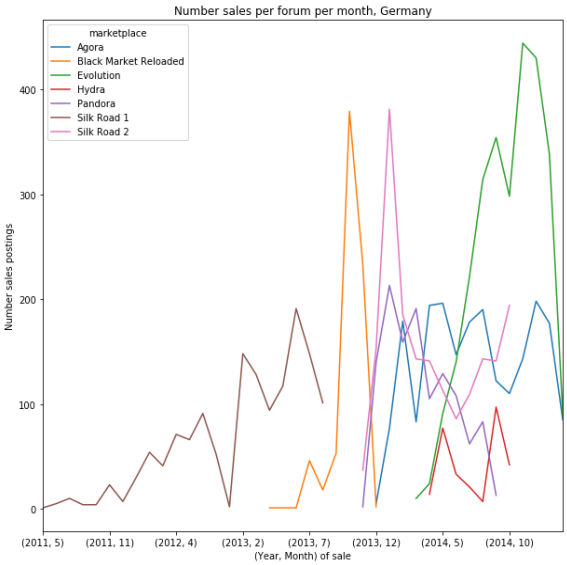


Figure 1: Number of sales per month, Netherlands

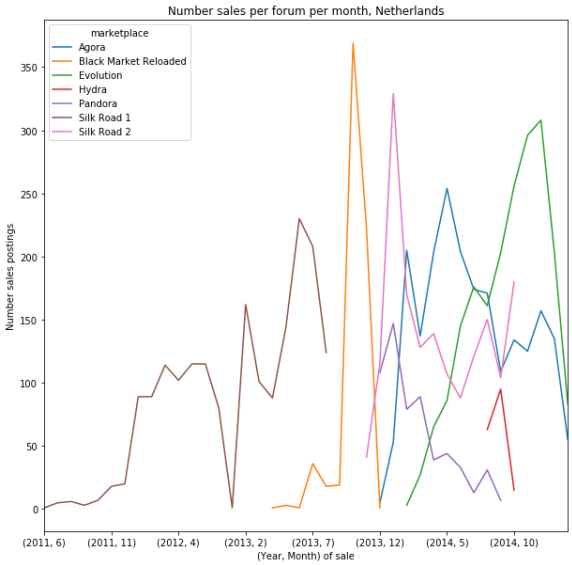


Figure 2: Number of sales per month, Germany

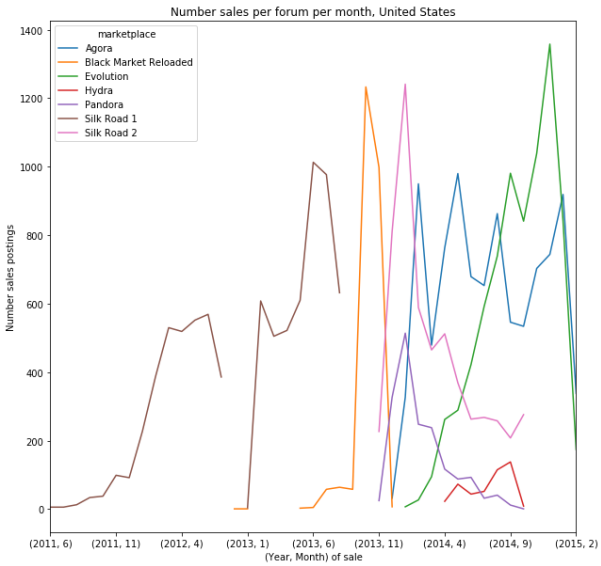


Figure 3: Number of sales per month, United States

## Total Sales per Month

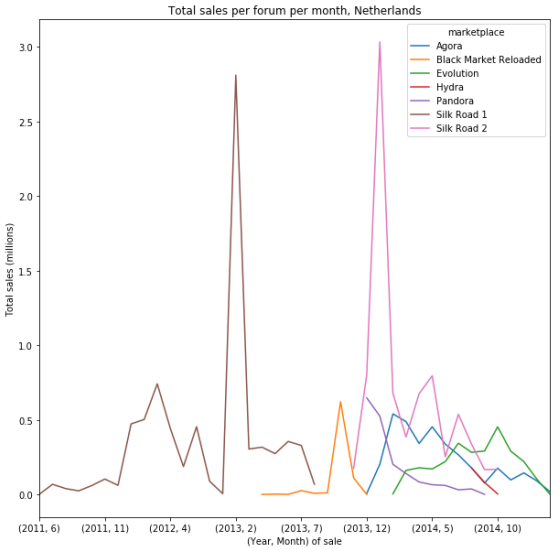


Figure 4: Total sales per forum, Netherlands

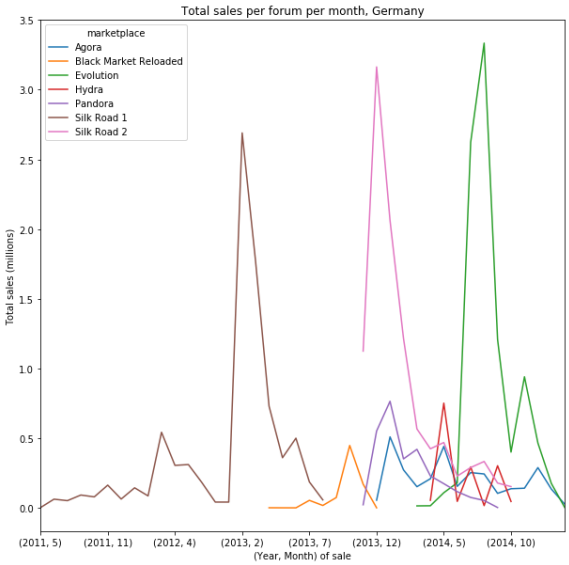


Figure 5:Total sales per forum, Germany

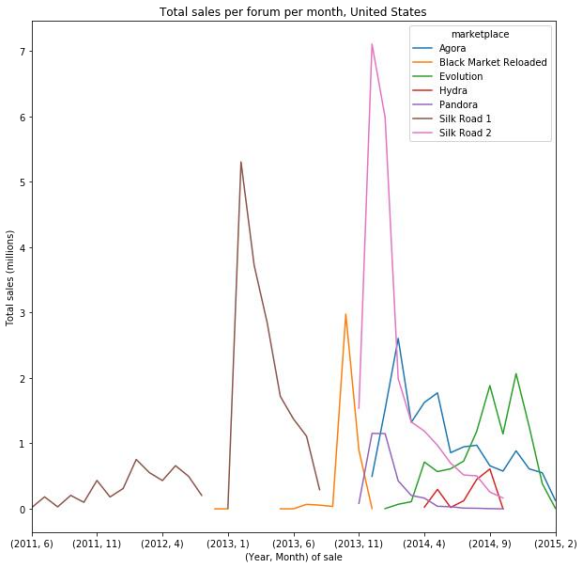


Figure 6: Total sales per forum, United States

The next step in analysing this data is to compare sales in each country. To do this, we have compared both sales totals and quantities of postings over time, normalized for the number of internet users per country. Normalizing based on internet users and not total population gives us a better idea of the number of sales per person who can access cybercrime forums in the first place. Data on number of internet users per country was found through Internet Live Stats [1].

Figures 7 and 8 indicate that the Netherlands has, on average, a higher number of sales postings and total sales over the course of the collected data. Most notably, data peaks, which map to peaks in sales on Silk Roads 1 and 2, are significantly larger in the Netherlands than in both Germany and the United States. The comparison with Germany is significant because of the similarities between both countries. Both are members of the EU and have similar demographics. So, higher sales for the Netherlands as compared to Germany indicates lower performance on the part of law enforcement organizations in the Netherlands, including the problem owner in this study. The United States is used as a second point of comparison. Data from the United States is on average similar to that from Germany and includes even lower peaks than that which is found in the data from Germany. Common metric

results from Germany and the United States, paired with significantly higher values from the Netherlands, indicate potential opportunity for improvement in security by law enforcement agents in the Netherlands.

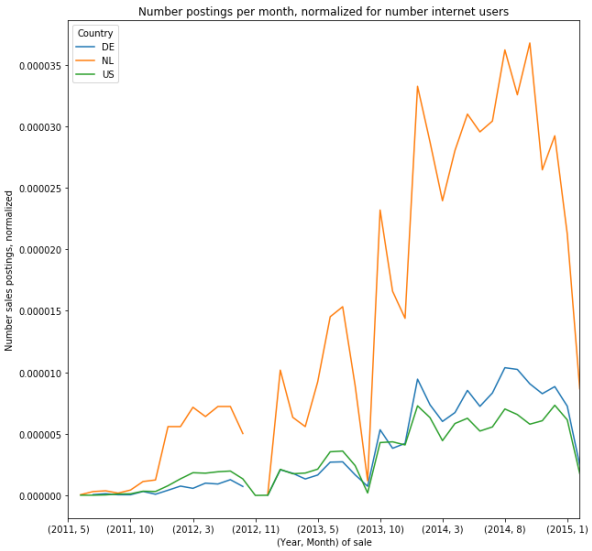


Figure 7: Number of postings per month, normalized

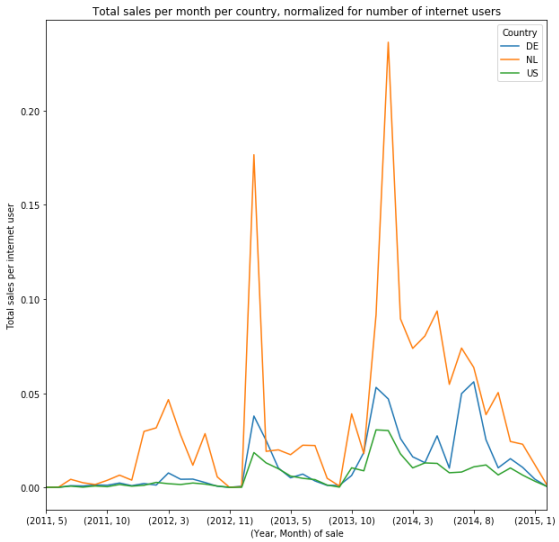


Figure 8: Total sales per month, normalized

Of note is the sharp drop shown in the last data point in these figures is more likely due to an incomplete set of data gathered for that month, and not a steep decline in sales.

# 4 Other Actors

In this section, several other actors will be discussed who are able to influence the security of a specific country. These actors are able to influence the sending and receiving locations of a transaction to some extent.

*Forum sellers*
Sellers on the forum are the supply side of the (illegal) goods offered. The sellers are individuals who operate from a certain location and it may be hard for them to relocate. Thus, the country from which the goods are shipped is not so much influenced by the sellers. On the other hand, the forum data shows most sellers do include a specific list of countries to which they ship their merchandise. This is likely influenced by their experience of the delivery rates (as this is mentioned in some cases). Changes in the countries to which a seller sells are easily influenced by their decision and thus contributes towards the metric of the receiving country. Also, note that the choice of a seller for a specific forum largely depends on the popularity of it among the buyers and its reputation.

*Forum buyers*
On the forums, buyers are the demand side of the market. In contrast to the sellers, they are not tied to the country the goods are shipped from but are limited to the country to which they are send. Note however that the availability to send goods to a country always depends on the sellers. The buyers therefore do not directly influence the security metric of a country but may to some extent influence sellers to make their product available to a country as there is demand. In the same way, the sellers choose a specific forum, the buyers are also interested in the forum with a better reputation.

*Forum owners*
The forums themselves are operated by forum owners. As they generate revenue based on the transactions conducted on their platform, there is an interest to keep the forum online with a good reputation. As such they try to keep scammers away and protect the anonymity of buyers and sellers. Individual forums are able to forbid certain types of goods; firearms are a good example of such a category which is forbidden in several forums. Although in the same way it is possible to forbid the advertisement of goods from or to a certain country, this was not done in the forums analysed. Thus, the forum owners are able to influence the export/import of goods for a certain country, but this is not done in practice.

*Law Enforcement agency of a different country*
As other countries may also take action on transactions going on within cybercriminal markets, this may result in not just a reduction of goods to their own country but in general. This is due to the fact that a single forum may not focus on a single location or language. Any action taken against the forum will then impact all buyers and sellers, regardless of the country they sell from. Another way a LE agency can have an influence is by arresting sellers from their country. This results in a lower supply side and will decrease the volume of transactions going on in the forums.

# 5 Risk strategies

Risk management related to the field of information security involves "the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk" [2]. The early NIST interpretation indicates, that risk management in the cyber field is working towards an acceptable level of risk. Linking back to the conclusion of our first assignment, that it is nearly impossible to fully eliminate cybercrime, it is important to come up with a sufficient strategy to manage the risk of cybercriminal markets.

## 5.1 Risk strategies for the Dutch National Police

There are four instruments that are used to determine strategy for cyber risks [3]. These four instruments are: risk reduction, risk acceptance, risk avoidance and risk transfer.

*Risk reduction.* Reduction tries to mitigate the likelihood and severity of loss event by protecting vulnerable assets with technical and organizational measures. However, the optimal level of information security investment does not mitigate the risk completely because at some point, the extra costs of more protection exceed the expected losses without that protection. As a result, there remains residual risk to be managed.

The Dutch National Police could use the following risk reduction strategies:

- Taking down cybercriminal markets as to disrupt the market and make it harder for buyers and sellers to find each other
- Monitor the different cybercriminal markets
- Outsource investigation of the cybercriminal markets to institutions and universities to gather information.
- Interrupt the trust chain as this may result in the less willing buyers to complete a transaction
- Create a fake underground market in order to get information of the cybercriminals (users who trade in illegal goods or services on the underground markets)
- Arresting the cybercriminals

*Risk acceptance.* The decision to tolerate losses, based on estimated risk (otherwise it can be interpreted that the risk was overseen rather than accepted). The propensity to accept information security risk depends on the core business, which sets bound for acceptable information. However, some risk cannot be accepted because it would break the law and this is in most of the cybercriminal market cases. The illegal trade on cybercriminal market break down the law and the duty of the national police is to protect the Dutch citizens and investigate the crime. Still, due to the limited manpower and cost the national police would have to accept some cybercriminal market trade, because they cannot investigate them all.

The Dutch National Police can use the following risk acceptance strategies:

- Focus investigation and operation on shutting the larger cybercriminal markets in terms of money flow rather than smaller cybercriminal markets.
- Once an underground forum is penetrated, target the focus of investigation and capture on large sellers, rather than the forum itself.

*Risk avoidance*. Implies that the organization withdraws from a risky business altogether. The cost of risk avoidance are forgone profits from the risky activity. In this case, the Dutch National Police has a legal obligation to citizens of the Netherlands to reduce criminal activity, so risk avoidance is not a possible strategy for risk management.

*Risk transfer*. The contractual agreement of financial compensation for uncertain future losses incurred due to the realization of risk. Transfer of risk can be accomplished through insurance or other contractual agreements that transfer liability to another organization. However, the transfer of liability is limited to what is legally permissible [4].

Sales of physical goods on cybercriminal markets, which represent a large portion of total sales transactions, lead to real-world movement of illegal goods. As an option of risk transference, The Dutch National Police can provide additional funding to border control and shipping organizations to increase their detection and security measures. In this way, the Dutch National Police have transferred some of the risk of illegal sales on cybercriminal forums to other governmental and private organizations. However, due to the obligations of the Dutch National Police to protect citizens of the Netherlands, they are limited legally in the amount of risk that can be transferred.

## 5.2 Risk strategies of other stakeholders

As identified in chapter 4, apart from the Dutch police, there are other actors who are also interested in influencing the cybercriminal activities through underground forums. When analysing different security performance metrics, it is important to view risk management strategies through different perspectives. This chapter will introduce the risk strategy proposed by other stakeholders, to continue building a foundation for calculation of return on security investment.

As Holt and Smirnova mention in [5], there is no easy or immediate way to disrupt or deter offenders engaged in cybercriminal markets. Therefore, it is suggested to come up with a global cybersecurity approach with individual targets that involves not only our problem owner, but a multilateral group of organizations. To accomplish this, a range of policy implications should be taken into consideration to increase the efficiency of law enforcement responses. As Ghernouti-Hélie proposes in [6], national leadership should ensure the cybersecurity action plan receives government-wide attention. To do so, their policy strategy should contain three domains:

- Ensure justice and police efficiency on a national level that is compatible for international strategy for a global perspective
- Develop a Cybersecurity culture and to raise awareness among citizens
- Ensure cybersecurity capacities with organizational structures, using technical and procedural solutions as well as human resources

*Risk strategy against forum sellers*
As mentioned in chapter 4, sellers on the forum are the supply side of the (illegal) goods offered. As cyber criminals usually take advantage of the lack of effective law enforcement, the Dutch police can partner with other organizations to:

- Increase the level of effort criminals must make to conduct a crime through enforcing managerial and technical security measures
- Increase the level of perceived risk and level of risks taken by cyber criminals though justice and police measures. Through legislative and regulatory measures, the perceived level of risk to the criminal can be increased and his motivation to pursue crime to be decreased. To accomplish this goal, it is necessary to build capacity in a coordinated and complementary way to ensure effective and operational legal, technical procedural and organizational measures.
- Decrease perceived expected profits to the forum sellers [6]

*Risk strategy against forum buyers*
To come up with a strategy against forum buyers, it is necessary to understand why they are interested in buying illegal products. By looking at their motivation, their correlation, tools and mode of action appropriate risk strategies can vary on their objective. As analysed in chapter 4, forum buyers are independent of their location and are interested in forums with good reputation.

*Risk strategy against forum owners*
Forum owners conduct revenue based on the transactions conducted on their platform. By addressing the payment methods used by the cybercriminals, the forum owners can be targeted, as suggested by Holt and Smirnova [5]. As suggested by various studies, most of the time criminals rely on only a few payment methods, some are

advertised specifically by the underground forums themselves, such as WebMoney. By examining the transactions on these payment methods, the efficiency of the market can be reduced, affecting the forum owners' revenue.

*Risk strategy working with Law Enforcement agencies of a different country*
The paper by Holt and Smirnova [5] identifies the lack of international strategic partnerships in tracking and hindering cybercriminal activities as a key weakness; suggesting investigation in international payment services to both increase transparency of investigation and increased connection between else compartmentalized enforcement agencies. However, while this strategy may slow down the flow of money, it might not disrupt the market as underground forum actors eventually will adapt to different strategies.

One approach to effectively disrupt the market and receive all buyer and seller cybercriminal data would be to establish forums unitedly with international law enforcement agencies. This strategy does not only target individual users, but a large scale of cybercriminals. It allows to track the behaviour of participants, to identify key buyers and sellers and to build use cases against entire networks of individuals. This strategy has been successfully employed during the "Dark Market" case. It not only ensures evidence against the criminal actors, but also distrust among them [5], [7].

### 5.3 Risk strategies of the other Stakeholders over time

In the early days of information security, the focus was on defending and closing every possible emerging vulnerability. Since then, the number of newly discovered vulnerabilities has been constantly growing, this strategy is considered no longer possible, as it is both too costly and impractical. Attacks come in many forms and attackers constantly evolve new tactics. Therefore, there has been a strategic shift in terms of information security from "fixing everything" and focusing on specific controls to narrowing threats. For this strategy, it is key to identify the most likely attack vectors and align the information security strategy to the most critical exposures. Frameworks, such as TARA imply methodologies to identify those exposures and to plan focus areas for security investments [8].

Cybercriminal forums represent an interesting case for addressing cyber risk over time. The nature of the underground forum means that a new forum is established almost immediately after an existing forum is taken down. This new forum then quickly takes the place of the old, with little impact on the sale of illegal physical and digital goods. Security actors addressing the risks of cybercriminal forums have historically focused on infiltrating and taking down the major forums. This has historically been proven true. As both national and international groups have taken down one forum after another, another forum takes its place and grows even larger than the one before it [9], [10]. Much of the work done by cybercriminal task forces to infiltrate and take down forums remains confidential. However, it is becoming clear that simply infiltrating and shutting down forums is not having a significant effect on reducing the amount of illegal sales on these forums. Figures 7 and 8 in chapter 3 demonstrate that a forum takedown has only a temporary effect on sales, and that the overall trend continues upward. These facts demonstrate that although efforts have been successful with respect to taking down underground forums, additional work and new strategies will be required to have a positive impact on the amount of cybercriminal activity on underground forums.

## 6 Return on security investment (ROSI)

The risk strategy that we will evaluate in this section, consists of infiltrating the online forum(s) to gather information of current transactions flows. The strategy will be separated into the different kinds of costs needed to setup this infiltration. We choose this strategy over just taking down forums, as in the already available data can be seen that old forums are replaced rather quickly. The result of this is that taking down a forum has a temporary effect. Infiltrating forums can have a lasting effect.

The risk strategy will be evaluated financially, since the budget investment of the National Police has to be justified and evaluated on its effectiveness. Assessing security investment involves evaluating how much potential loss could be saved by a certain investment. Therefore, the Return on Security Investment (ROSI) will be used to compare the monetary value of the investment with the monetary value of the risk reduction [11].

In the following two sections, the cost of the solution and the monetary loss reduction will be determined in order to calculate the ROSI in section 6.3.

## 6.1 Cost of the solution

Calculating the indirect costs is difficult, since they would have to be measured afterwards. It is assumed that the strategy will be implemented by a national Dutch National Police which already has several supporting facilities such as offices and a basic IT infrastructure

For the initial development and maintaining the platform, we estimate the cost in FTE (Full Time Equivalent) as this requires someone developing the software. The cost of 1 FTE is estimated at 65000 euro per year [12]. As the result of the gathered information is used as an input for prioritising different investigations, there is no cost associated with the investigation itself, since they are already being conducted.

*Sunk one-time costs*

- Training employees on setting up and using the monitoring platform. Specific knowledge is required in order to understand how the cybercriminal markets operate, how to infiltrate and gather information. Related trainings usually take 3 days and cost 2250 EUR per person [13]. The assumption is that there are two employees working on infiltrating forum. This enables them to partner and work more efficiently than a large team. Thus, the total *training cost* are 4500 euro.
- Initial development of the monitoring platform. In order to extract the data from the forums and provide a way to analyse this, a platform must be created. This result of this software project will provide users with an easy to use analytic tool to generate metrics based on the forums. It is estimated that this will cost 0.5 FTE, which makes 32500 euro.

*Recoverable one-time costs*

- IT hardware costs for the monitoring platform. As the monitoring platform needs computing resources to run, there are direct costs to buying hardware. If the project dissolved, these costs can be recovered by using the hardware in another project. This makes the costs recoverable. Assuming that the needed resources of the platform are quite modest, the cost of hardware is estimated at 2000 EUR [14].

*Recurring costs*

- Maintaining and developing monitoring platform. Given several forums will appear over the course of a year and integrating each of these might take some time, it is estimated that keeping the forums integrated and the software up-to-date will cost 0.2 FTE, thus 13.000 euro
- Employees working with the platform and infiltrating the forums. As most of the effort will go into building trust relations with other buyers and sellers, this human component requires that the police have enough employees on doing this. We estimate that 2 FTE is needed per forum, which makes 130.000 euro.

The total cost of the strategy, infiltrating forums (solution cost) is calculated in table 1.

Table 1: Cost of the Solution per employee

| **Solution cost** | **Euro** |
|---|---|
| Training cost | 4.500 |
| Monitoring Platform | 32.500 |
| IT Hardware | 2.000 |
| Maintaining/Developing monitoring platform | 13.000 |
| Employees working with the platform | 130.000 |
| Total cost | **182.000** |

It should be noted that the Dutch National Police is not the only actor with an interest in monitoring and infiltrating these forums. Several of the costs, mainly developing and maintaining the platform, could be shared among different countries who would all have access to the same platform. However, this is not included in above mentioned calculation.

## 6.2 Monetary loss reduction

The purpose of the risk strategy to infiltrate the forums is to reduce the illegal drugs-related transactions and result in a positive impact on the society. To determine the positive impact on the society, the cost of drugs on society will be defined and thereafter could be determined how much cost on the society will be eliminated due to the reduction of crime.

The National Treatment Agency for Substance Misuses calculated the cost of drugs on the public, businesses and criminal justice [15]. They divided the cost of drugs on the society into four categories: drug-related crime cost, the cost of a crime by an addicted person, cost of deaths related to drug misuse and the overall drug misuse cost. Thereafter, they calculate how much a prevented crime would save on the society. A prevented crime, due to drug prevention, saves an estimate of 188 pound in 2011. The average exchange rate in 2011 was 1,1624, thus this would be 220-euro savings for each prevented crime.

In ROSI, the estimated cost savings by preventing a crime could be defined as the *single loss*, which is the expected amount of money that will be lost when a risk occurs (SLE=220). The *single loss expectancy* times the *annual rate of occurrence* (probability that a risk occurs in a year) defines the annual loss expectancy. The annual rate of occurrence is estimated by the amount of total sales on the forums, since an illegal transaction is the risk occurrence. The total amount of sales from all the forums which are shipped from the Netherlands to the other countries is 9.064 (ARO=9.064).

The annual loss expectancy times the mitigation ratio of the risk strategy is the monetary loss reduction. The assumption is that the risk strategy of infiltrating forums would reduce the sales between 10 – 25 %. We assume the "worst-case" scenario that infiltrating the forums will reduce the sales with 10% (Mitigation ratio=10%). The monetary loss reduction is defined as follows:

$$Monetary\ Loss = SLE * ARO\ * Mitigation\ Ration$$
$$Monetary\ Loss = €220 * \ 9.064\ * 10\% = \ €199.408$$

## 6.3 Calculation ROSI

As mentioned above, the ROSI will be used to compare the monetary value of the investment with the monetary value of the risk reduction and is defined as followed:

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

The *cost of the solution* is calculated in section 6.1 and the *monetary loss reduction* in section 6.2. This enables us to calculate the return on investment (ROSI):

$$ROSI = \frac{199.408 - 182.000}{182.000} = 0{,}0956$$

According to the ROSI calculation, the risk strategy of infiltrating the forums is a cost-effective strategy, since it generates a positive output.

# 7 Conclusion

The existence of cybercriminal marketplaces represents a significant security threat to the Dutch National Police, and requires a complex risk management strategy to address. by analysing past data of sales posts on these forums and comparing the results of other similar countries, the effectiveness of existing policy in this area can be examined. In this case, there have been a higher number of sales, both in number and normalized for internet users in country, in the Netherlands as compared to Germany and the United States. This indicates a possible shortcoming in current policy for the Netherlands and the Dutch National Police as compared to relevant stakeholders in other countries.

By examining potential risk management actions that fall under four categories, reduction, acceptance, avoidance, and transfer, as well as the potential risk management actions of other actors, and trends in risk management

strategy over time, an updated comprehensive risk management strategy can be developed. Finally, the return on security investment (ROSI) calculation, which involves determining the return on investment of a security strategy by analysing the assumption-based costs and benefits of that strategy, can provide guidance as to the effectiveness of the strategy. This analysis can be further extended beyond this assignment to compare the return on multiple strategic options, which can enable the Dutch National Police to make the most effective decisions when managing the risk that exists from cybercriminal marketplaces.

In this case, a strategy that focuses on infiltration of cybercriminal forums, monitoring of major sellers, and impacting their sales. This strategy was selected because it focuses on interrupting the sales cycle, rather than focusing on taking down forums, as past data has indicated that forum takedown does not lead to a lasting reduction in cybercriminal activity. The conclusion of that analysis is that infiltrating the online forums to gather information of current transactions flows, is a cost-effective risk strategy and is therefore needed to invest in.

# 8 References


[1] Internet Live Stats, "Internet Users by Country (2016)," 2016. [Online]. Available: http://www.internetlivestats.com/internet-users-by-country/. [Accessed: 08-Oct-2017].

[2] ENISA, "Technical Guideline on Security Measures," 2014.

[3] B. Guttman and E. A. Roback, "SP 800-12. An Introduction to Computer Security: the NIST Handbook." National Institute of Standards & Technology, 1995.

[4] CNA, "Risk Transfer: A Strategy to Help Protect Your Business," 2016.

[5] T. J. Holt and O. Smirnova, "Examining the Structure, Organization, and Processes of the International Market for Stolen Data Examining the Structure, Organization, and Processes of the International Market for Stolen Data Award Number: 2010-IJ-CX-1676," 2014.

[6] S. Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture," in *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 370–373.

[7] K. Poulsen, *Kingpin : how one hacker took over the billion-dollar cybercrime underground*. 2012.

[8] M. Rosenquist, "Prioritizing Information Security Risks with Threat Agent Risk Assessment," 2009.

[9] K. Leswig, "The FBI just took down AlphaBay, an online black market for drugs that was 10 times bigger than Silk Road," *Business Insider*, 20-Jul-2017.

[10] A. Greenberg, "End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market," *Forbes*, 02-Oct-2013.

[11] Enisa, "Introduction to Return on Security Investment," no. December, p. 18, 2012.

[12] Politiedienstencentrum, "Vacature technisch informatieanalist business intelligence." [Online]. Available: https://www.kombijdepolitie.nl/Vacatures/Paginas/technischinformatieanalistbusinessintelligence_1927535.aspx. [Accessed: 08-Oct-2017].

[13] Fox-IT Delft, "Cybercrime; Attack & Defend." [Online]. Available: https://www.fox-it.com/academy/module/monitoring-security-analist-1/cybercrime-attack-defend/. [Accessed: 08-Oct-2017].

[14] Dell, "PowerEdge Rack Server Deals," 2017. [Online]. Available: http://www.dell.com/nl-nl/work/shop/deals/enterprise-deals/poweredge-rack-server-deals. [Accessed: 08-Oct-2017].

[15] NTA, "Why invest? How drug treatment and recovery services work for individuals, communities and society," London, 2011.