Cybercriminal Markets

Economics of Cyber Security Assignment Block 3 - DRAFT

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

Delft University of Technology

Abstract.

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.

2 Problem Owner of Security Issue of Cybercriminal Markets

The security issue of cybercriminal underground markets is the trade in illegal products, such as drugs, that might be result in violence and thereby harm the Dutch citizens' well-being. The problem owner of this security issue is the Dutch national police, which focus on the national security and the protection of the citizens.

The security issue of cybercriminal underground markets is the trade in illegal products, such as drugs, 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 Indication of Current of 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 the figures below. 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

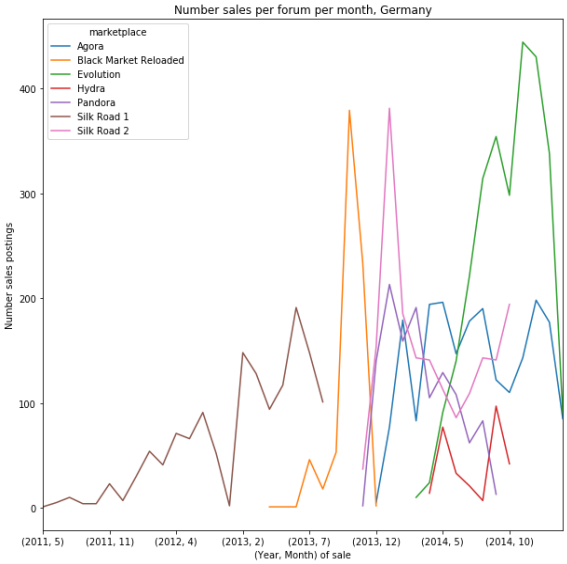


Figure 1: Number of sales per month, Netherlands

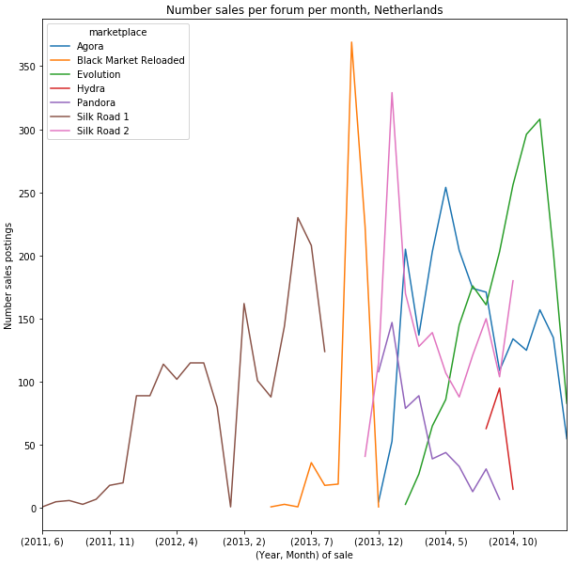


Figure 2: Number of sales per month, Germany

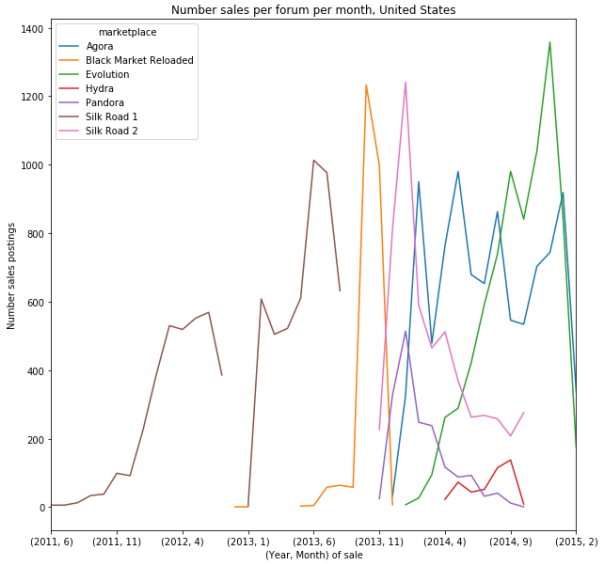


Figure 3: Number of sales per month, United States

Total Sales per Month

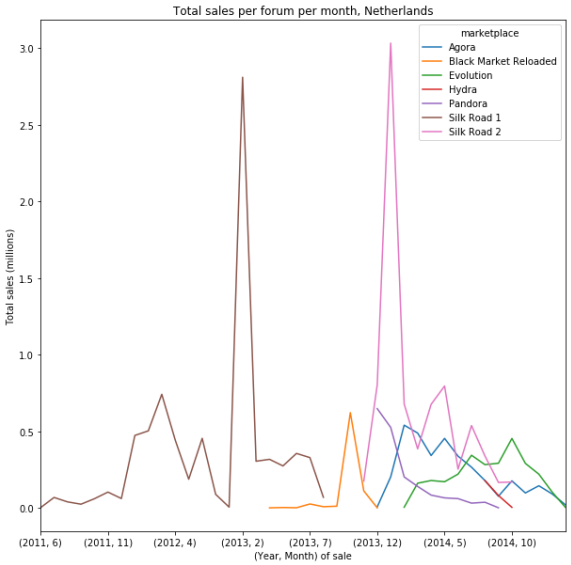


Figure 4: Total sales per forum, Netherlands

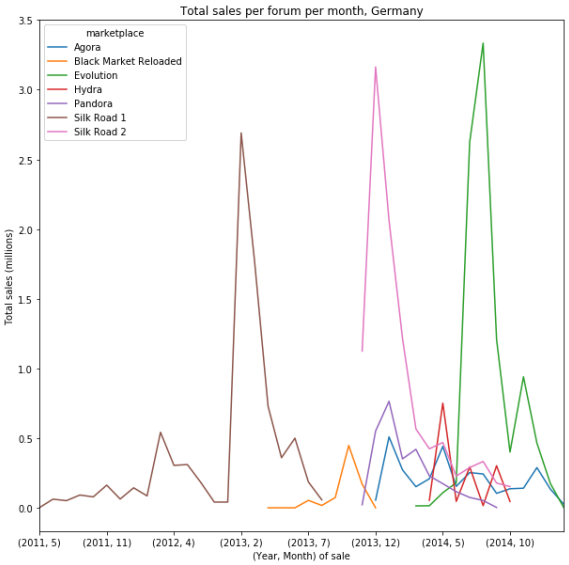


Figure 5: Total sales per forum, Germany

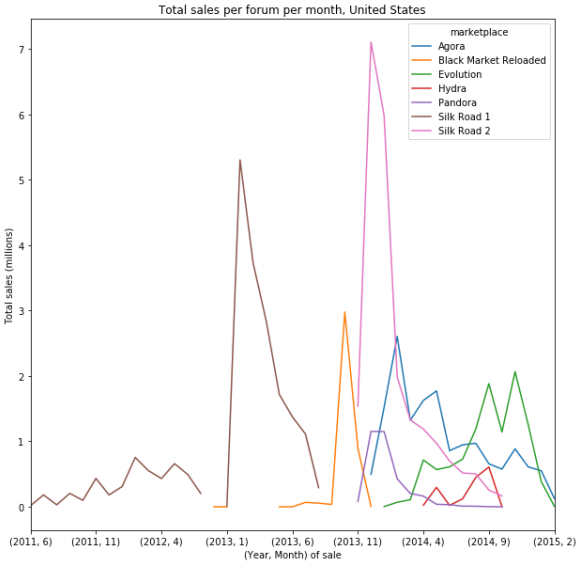


Figure 6: Total sales per forum, United States

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 here: http://www.internetlivestats.com/internet-users-by-country/)

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.

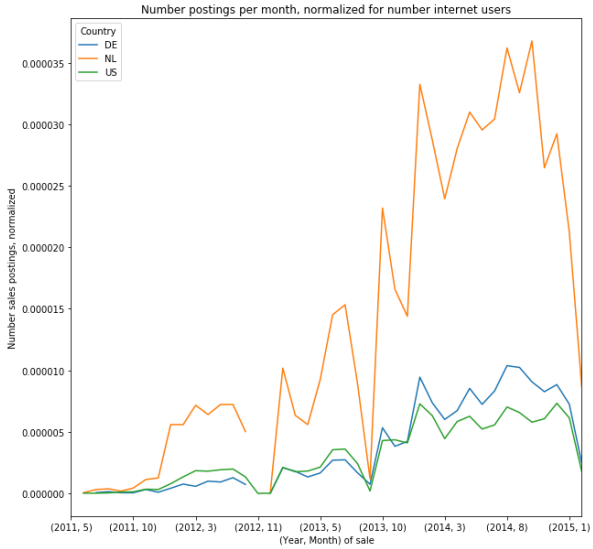


Figure 7: Number of postings per month, normalized

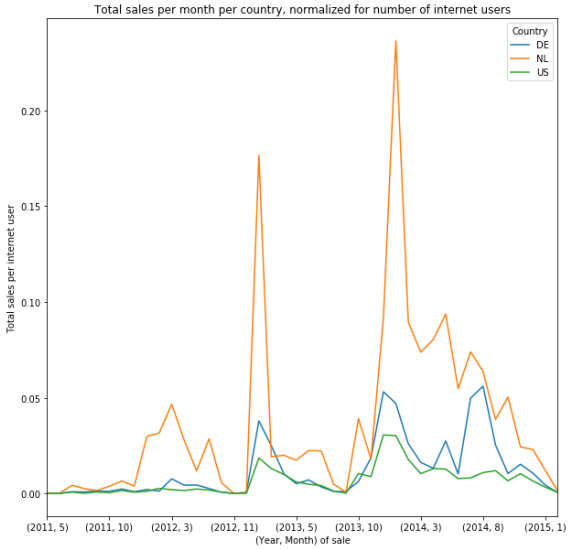


Figure 8: Total sales per month, normalized

4 Other Actors

In this section, several other actors will be discussed who are able to influence the security of a specific country. All of these 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 analyzed. 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 can 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 ex ante (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 strategy:

- The focus of investigation and operations to shut the markets down rely on the larger cybercriminal markets in terms of money flow rather than the smaller cybercriminal markets.

Risk avoidance implies that the organization withdraws from a risky business. The cost of risk avoidance are forgone profits from the risky activity.
Risk transfer is the contractual agreement of financial compensation for uncertain future losses incurred due to the realization of risk.
Both risk strategies; avoidance and transfer would be unlikely to use by the Dutch National police, since the law-enforcement purposes of the police are the investigation of suspected criminal activity and this would imply that the police do not conduct their jobs.

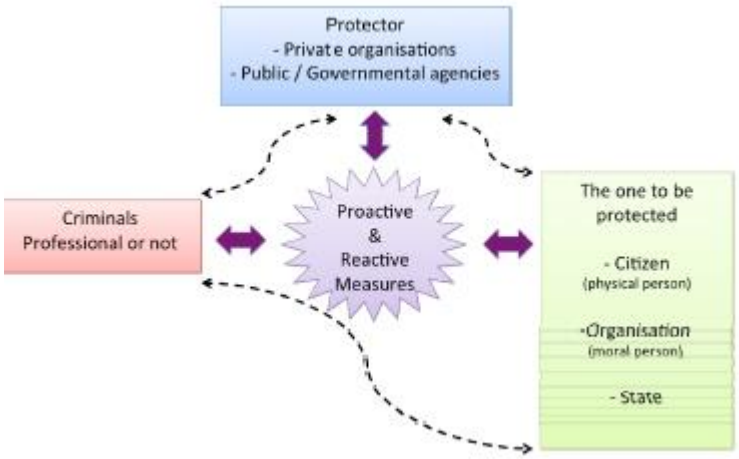
5.2 Risk Strategies of the other Stakeholders

As identified in chapter 3, apart from the Dutch police, there are other actors, who are also interested in influencing the cybercriminal activities through underground forums. When analyzing different security performance metrics,

it is important to view risk management strategies through different perspectives. However, the problem mainly needs to be addressed through a nation or global security strategy to be able to equally address the security of individuals. This chapter will introduce the risk strategy proposed by xx as foundation for further return on security investment analysis.
[1] proposes, that 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

[1] Identifies two categories of security strategies, depending on how they are preceded: pro-active and reactive security.



5.3 Risk Strategies of the other Stakeholders over time

Have the strategies changed significantly over time in a way that reduces or increases risks?

In the early days of information security, the focus was on defending and closing every possible emerging vulnerability. Ever since the number of newly discovered vulnerabilities has been ascending, this strategy is considered as no longer effective, 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. [4]

6 Security Performance Metrics

tdb

1. **What relevant differences in security performance does your metric reveal?**
   Difficult to do with our data.
   Idea: compare incidents normalized to population (adults or **internet users** or total population) of countries with similar populations and with different populations. Fewer incidents means actions are working. More incidents means there is a place to look for better control ideas. - Erin
   Do we just focus on one metric for question 2?

7 Return on Security Investment of xxx

tdb

1. **Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,**
   Estimate the costs involved in following that strategy
   Estimate the benefits of following that strategy (assume a particular loss distribution)
   In order to measure the Return on Investment
   If we would focus on the cost of drugs for the national government it is not related to cyber risk? The items database differentiates between multiple kinds of drugs, Misc, other, and digital goods, with no definitions about what is included in digital goods.
   Calcualte additional metrics + reflection of the metrics how they are on the security issue expalaory analyisis -> WHY there are differences
   Use database to pick the strategy
   http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_19-1.pdf
   https://www.ftc.gov/system/files/documents/public_comments/2015/10/00027-97671.pdf

In order to justify the investment in risk strategies to prevent cybercriminal activities via underground forums

https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport

Return on Security Investment (ROSI)

Following the ROI definition, the ROSI is defined as below:

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

Implementing an effective security solution lowers the ALE: the more a solution is effective, the more reduced is the ALE. This *monetary loss reduction* can be defined by the difference of the ALE without the security solution versus the modified ALE (mALE) implementing the security solution.

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

Which also equals to the *mitigation ratio* of the solution applied to the ALE:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

In their study, the authors state that, contrary to the basics of risk assessments, an asset of greater value should not necessarily benefit from a greater investment to protect it. The optimal information security investment does not always increase proportionately to increases in vulnerability; there is a point at which it is not in the best interest of a firm to make increasingly larger investments in information security.

According to this study, "*the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach (and is typically much less that 37%). Hence, the optimal amount to spend on information security would typically be far less than even the expected loss from a security breach*".

8 Conclusion

tbd

References

[1] S. Ghernouti-Hélie, "A national strategy for an effective cybersecurity approach and culture," *ARES 2010 - 5th Int. Conf. Availability, Reliab. Secur.*, pp. 370–373, 2010.

[2] B. Guttman and E. Roback, "An Introduction to Computer Security : The NIST Handbook," *Natl. Inst. Stand. Technol. Technol. Adm. U.S. Dep. Commer. An*, vol. SP800, no. 12, pp. 1–278, 1995.

[3] J. F. Al-Bahar and K. C. Crandall, "Systematic Risk Management Approach for Construction Projects," *http://dx.doi.org/10.1061/(ASCE)0733-9364(1990)116:3(533)*, vol. 116, no. 3, pp. 533–546, 1990.

[4] Intel Information Technology, "Prioritizing Information Security Risks with Threat Agent Risk Assessment." p. 8, 2009.