# WM0824TU
# Economics of Cyber Security

## Group 5 – Assignment 2

## 28 September 2015

## Overview

# 1. What security issue does the data speak to?

PhishTank and Clean-mx provide data on phishing: from locations of compromised servers to URLs of phishing websites. According to Moore & Clayton (2007), phishing can be defined as follows:

*"Phishing is the process of enticing people into visiting fraudulent websites and persuading them to enter identity information such as usernames, passwords, addresses, social security numbers, personal identification numbers (PINs) and anything else that can be made to appear to be plausible. This date is then used to impersonate the victim to empty their bank account, run fraudulent auctions, launder money, apply for credit cards, take out loans in their name, and so on."*

It is obvious that possessing such personal data opens many possibilities for financial crimes. According to Gartner (2007), about 3 billion dollars was lost by phishing attacks in 2007, with an average loss of $886 per incident. The most often attacked brands are PayPal and eBay, both involved in many financial transactions and used by a great amount of customers, which makes them very attractive targets.

Since phishing is one of the most lucrative cybercrimes, policy makers should develop a strategy to combat these criminal activities. This policy can be aimed at different stakeholders, such as:

- Internet Service Providers (ISPs): they should make sure that confirmed phishing URLs are blocked;
- E-mail providers: they should make it very difficult for phishing e-mails to pass through the spam filter;
- Banks and other institutions that can be spoofed: they should have clear safety policies and make it hard for phishing criminals to imitate their systems;
- Users of the services of these institutions: they should be aware of phishing tactics so they do not fall easily for the fake e-mails and websites.

In order to get more insight in the problem of phishing, to know what policies are most effective and efficient, and to come up with new, better policies, it is required to be able to measure various aspects of phishing. What aspects of phishing are crucial for the profitability and thus the existence of this crime? In this assignment, metrics will be proposed to measure these aspects.

### Focus on targeted countries

This assignment will cover metrics regarding the countries that are targeted by phishing websites. What countries are more "popular" or vulnerable to attack and why could that be? How well do they succeed in bringing down the websites? Although there are many more issues within phishing that are interesting to address, this is a good starting point. Information on the attacks targeted at a country can show the development of phishing in a country, which can be a base for policy changes. Also, in retrospect, this focus is well achievable with the data available.

First, ideal metrics on phishing in a targeted country for security decision makers are designed. In this first step the actual availability of data in practice is not taken into account yet –pretending all data to make good policy decisions is available. Unfortunately this is not the case at all. Therefore the metrics that exist in practice are observed. Lastly, the datasets of PhishTank.com and Clean-mx will be examined to assess what metrics can be derived from it.

**Discussion**

Other focusses could also be very interesting – for example basing analyses on the country of origin might provide insight in the concentration of criminal organisations, but due to e.g. botnets this is hard to track. Analyses based on business sectors could be able to provide insight on the "popularity" of certain industries, like PayPal and eBay – financial transaction services – that were most targeted in 2007 (Gartner, 2007). However, all known targets should then be categorized into business sectors, which is certainly feasible but not in the time scope of this assignment. Appendix A contains the metrics resulting from a brainstorm that included multiple focusses. This brainstorm was used for background research and scoping.

## 2. What would be ideal metrics for security decision makers?

The main purpose of metrics is to compare between alternatives. These metrics should provide useful information regarding security-related objectives.

Rainer Böhme introduced a framework that covers the different components of decisions on security: 'cost of security', 'security level' (which together determine the security productivity curve) and 'benefit of security' *[Böhme, R. (2010)]*. By estimating the values of these different components, one can use them to enlighten the organisation by showing some type of progress. The organisation then can determine if action is needed or if there are changes to be made.

The estimations require a lot of data. Data regarding costs and benefits are usually internal data from a specific company. One has to know about the spendings of a company to determine the direct and indirect 'costs of security' and data about the results of these costs to determine the 'benefit of security'. Since this kind of data is hard to get, this paper will focus on the 'security level' aspect. Usually data regarding the security level is easy to obtain. This data can contain information about for example the amount of attacks and success rates of these attacks.

Some metrics are better than others. The key to good security metrics is obtaining measurements that satisfy the following statements:

- Metrics should contain relevant information;
- Metrics should be reproducible;
- Metrics should be objective and unbiased;
- Over time, they should be able to measure some type of progression towards a goal.

Some metrics count items of a certain aspect in a region. For example, the amount of attacks in a country. These metrics by itself can be biased since the amount can be influenced by different factors. Therefore, to make these metrics more meaningful, they must be normalised. This way the influences of a certain factor are eliminated. For example, the amount of attacks per country can be heavily influenced by the amount of internet users per country. By dividing the amount of attacks by the amount of internet users, a measurement is derived which is unbiased towards the internet community of the country.

## Ideal metrics conducted from brainstorm and literature

| **Metric** | **Explanation** | **Theoretically feasible or not** | **If not feasible, why?** |
|---|---|---|---|
| **Uptime of phishing website per** targeted country | Shows for how long the website has been online differentiating from country to country. It could be useful to analyse the suppression response of the various countries in order to evaluate their law enforcement. | Feasible. | |
| **Money lost per incident/country/target/time** | Shows the amount of money lost due to phishing in the various dimensions. | Feasible/ unfeasible.<br>Reference: ”Measuring the cost of cybercrime”, 3.2 online banking fraud | It’s hard to determine the exact amount of money lost per incident. In some case the loss could be indirect. Also not every data is available.<br>It has been estimated. |
| **Number of internet users per targeted/origin country** | Useful to give a proper weight to country-based metrics.<br>(Trivial Information) | Feasible. | |
| **GDP per targeted/origin country and presence of normalised targeted phishing** | It could be interesting to study whether there is a correlation between a country’s wealth and attacks.<br>(Trivial Information) | Feasible. | |
| **Distribution of attack goals per targeted country** | Shows whether different countries have different phishing problems.<br>E.g. countries with more modern economy could suffer more from home banking phishing rather than other kind of phishing. | Not feasible. | Not all information is available.<br>Also multiple goals can be pursued with a single attack. |
| **Number of attacks per country/region, normalised by the number of local internet users** | Shows where phishing (as origin and targeted country) happens more/less. The metric should be normalised accordingly to the number of internet users of that country/region. | Feasible. | |
| **Number and distribution of mules per country, normalised by the numbers of local internet users** | Shows how many mules are present in the country. This metric should be normalised accordingly to the number of internet users of that country/region. | Not feasible. | The exact number of mules is really hard to measure. Data are scarce. It could be estimated. |
| **Number of phishing emails received pro capita per country, per time unit** | Shows how many emails a person receives on average per specific country in a determined period of time (a day, a week, a month, a year etc.). | Feasible, using for example data from ISPs and mail providers | |
| **Amount and size of criminal phishing organisations per country** | Shows how many criminal organisations related to phishing exist in different countries. This value is useful both normalised to the number of Internet users of that country (or even the general population) and not normalised. | Not feasible. | It's hard to have exact data related to specific criminal organisations. |

## 3. What are the metrics that exist in practice?

In practice, most metrics are not as specific as in an ideal situation. They do not discriminate between business sectors, amount of internet users per area, and so on. It is obvious that the main goal of phishing information clearinghouses, like phishtank.com, is merely to expose phishing sites. Although sometimes it is possible to search for certain variables such as “target” and “country”, performance variables such as uptime are not kept track of consistently. It is therefore hard to retrieve an extensive database on which research can be conducted.

The variables, and therefore the conductable metrics, of phishing detection sites are based on incidents. They are hard to interpret without knowledge of underlying, sometimes hidden, causal relationships. The examples below are incomplete in that sense, since normalisation or underlying causalities are not taken into account.
Although no useful conclusions can be derived from these metrics, it does show that these phishing clearinghouses focus on measuring the prevalence and severity of phishing sites. One similar example of the use of such measures was found in literature (Doshi et.al., 2006).

PhishTank.com (2015) and Clean MX (2015) deliver data on the following statistics:

| PhishTank | Clean MX | Doshi et.al. (2006) |
|---|---|---|
| • Phishes Verified per Day<br>• Phishes Submitted per Day and per Hour<br>• Total Phishes Submitted / Valid / Invalid per month<br>• Median Time to Verify (by the community)<br>• Top 10 domains of valid phishes<br>• Top 10 IP addresses of valid phishes<br>• Top 10 Networks that host phishes<br>• Popular Targets | • Phishes detected and closed per Day<br>• Distribution of % phishing sites worldwide and per country<br>• Nameserver distribution worldwide and per top 25 countries<br>• Phishingsite distribution top 25 countries, per region | • Average Phishing URLs Per Day<br>• Distribution of Obfuscation Types Used<br>• Average Phishing Victims Per Day<br>• Distribution of Phishing by Organization<br>• Geographical Distribution of Phishing |

The Anti-Phishing Working Group (APWG, 2015) seems to do a somewhat better job in their quarterly reports. Some of their metrics actually do make distinctions on important factors such as industry sectors, or contribute to more insight when combined with other metrics.

| Not specific | More specific |
|---|---|
| • Number of unique phishing websites detected<br>• Number of unique phishing e-mail reports (campaigns) received by APWG from consumers<br>• Contain some form of target name in URL<br>• No hostname; just IP address<br>• Percentage of sites not using port 80<br>• Phishing by top-level domain<br>• Malware infected countries (ranking between countries, and type of malware)<br>• Measurement of detected malware | • Most targeted industry sectors *(discriminates between industrial sectors)*<br>• Countries hosting phishing sites *(instead of looking at attacked countries)*<br>• Phishing-based Trojans and Downloader’s Hosting Countries (by IP address)<br>• Number of unique brands targeted by phishing campaigns *(instead of a total amount of attacks, this helps to provide insight in the distribution of attacks over brands).* |

Apart from the above examples of incomplete incident metrics, another phishing related type of metric is found in literature. This is about how well a technology is capable of recognizing phishing sites or e-mails. These metrics are based on controls and their performance and have some overlap with each other.

Performance metrics found in literature include:

- False positive rates (DeBarr et.al., 2013; Miyamoto et.al., 2008; Wardman, 2014);
- Area Under the receiver operating characteristic Curve (AUC) (DeBarr et.al., 2013; Miyamoto et.al., 2008) which measures accuracy;
- F(1) measure (DeBarr et.al., 2013; Miyamoto et.al., 2008) which can be seen as a weighted average of precision and recall;
- Precision, accuracy and recall (DeBarr et.al., 2013).

Searches in databases like Scopus and IEEE with search terms "phishing" and "metric*"only deliver one page with results – which is not much. When "metric*" is left out, suddenly over 5 pages of results come up. While it is never good to jump to conclusions, it does give food for thought regarding the status quo of experience and performance evaluation in phishing management.

## 4. What metrics can be derived from the data?

**Acquiring the research data**

Our research data consists of two sites: https://www.phishtank.com/ and http://support.clean-mx.de/clean-mx/phishing.php. These sites contain information about phishing sites, for example on the url, target and ip-state.

The first site, PhishTank, contains few information. One can only derive the url of the phishing website, if it is a verified phishing website and if it is still online. By clicking on an issue, one can also see technical details and a screenshot of the page itself. The data can be downloaded in useful formats such as XML or Csv, but since the data contains so few information, we didn't use this website.

The second site, Clean-mx, is a big source of information. It contains a lot of information about phishing websites, which are useful for defining and evaluating metrics. Data in this database is updated very frequently, which means the data is always up-to-date. The data is only downloadable in XML format.

But we stumbled upon some troubles using this data source. First of all, we acquired some weird data. The information of a phishing website contains 'up-time', the time the website was online. The data we acquired told us that almost every closed phishing website, had an up-time of either 24 hours or thousands of hours. This seemed strange, since the amount of closed phishing websites with an up-time of 24 hours was extremely high. But since this was our main source of data, we decided to still use it to evaluate our metrics.

The second problem we faced was as follows. When looking at the data from the site itself we could see that many phishing websites were closed. Therefore they also contained information about the up-time. But when downloading the data in XML file, we noticed that suddenly every phishing website was still open and therefore the information about up-time was gone. We concluded that the data from the site and the data in the XML file were not the same. But since the XML file still contained useful information, we decided to still use it to evaluate the metrics and copy the uptime data, which was not available in the XML file, directly from the site.

**Ideal metrics**

The ideal metrics that can be derived from the available data are: "Uptime of phishing website per targeted country", "Number of internet users per targeted country ", "GDP per targeted country and presence of targeted phishing", and "Number of attacks per country/region, normalised by the number of local internet users". Some underlying information is needed, like GDP and internet usage. This is not a problem (see Appendix B).

Unfortunately all other ideal metrics are not possible with the data available. For example, none of the phishing clearinghouses tracks the money involved in incidents and there is no raw data on the internet, except for a few generic reports like Gartner's. Also there is no way of tracking the motivation behind every attack to create a distribution; phishing clearinghouses do not include data on mules, there is no time to contact and negotiate with e-mail providers on the release of phishing e-mail data, and the amount and size of criminal phishing organisations is unknown.

**Definitions of feasible metrics**

1. *"Uptime of phishing website per targeted country"*
   Clean-mx provides information on the amount of hours it took from noticing a phishing website to closing it down. This is assumed to be the uptime. Obviously the phishing website must have been online before it was noticed, but since it is impossible to make a guess for that time, the uptime will be defined as the amount of hours from noticing to closing down. Averages will be constructed for fifteen countries to illustrate the use of the metric.

2. *"Number of internet users per targeted country"*
   This is an underlying metric that has to be calculated in order to normalise the amount of attacks per country.

3. *"Number of attacks per country/region, normalised by the number of local internet users"*
   The number of attacks is defined as the number of notified phishing websites on Clean-mx. Unfortunately, nowhere a definite amount is given. Therefore percentages are used from the Stats page to determine what share of attacks went to each country (Clean-mx, 2014). To compensate for large countries having more attacks, the amount of attacks is normalised for the amount of inhabitants who use internet and are thus potential prey to phishers. The number of internet users per country is taken from www.internetlivestats.com/internet-users-by-country/. Data are from 2014.

4. *"GDP per targeted country and presence of normalised targeted phishing"*
   In order to get an understanding of the wealth of a country's inhabitants – and thus their attractiveness to phishers – the GDP should be divided by the number of inhabitants, resulting in GDP per capita (Appendix B). GDP *nominal* per capita is used, not *purchase power parity (PPP)*, since the metric should be able to compare between countries. GDP nominal per capita reflects

the absolute level of wealth (in this case, in current US$), and is thus comparable to other countries. GDP PPP per capita reflects the GDP per capita in relation to e.g. the costs of living in a country, which shows whether the absolute GDP per capita actually results in a good standard of living within the country. This is not of interest to this study.

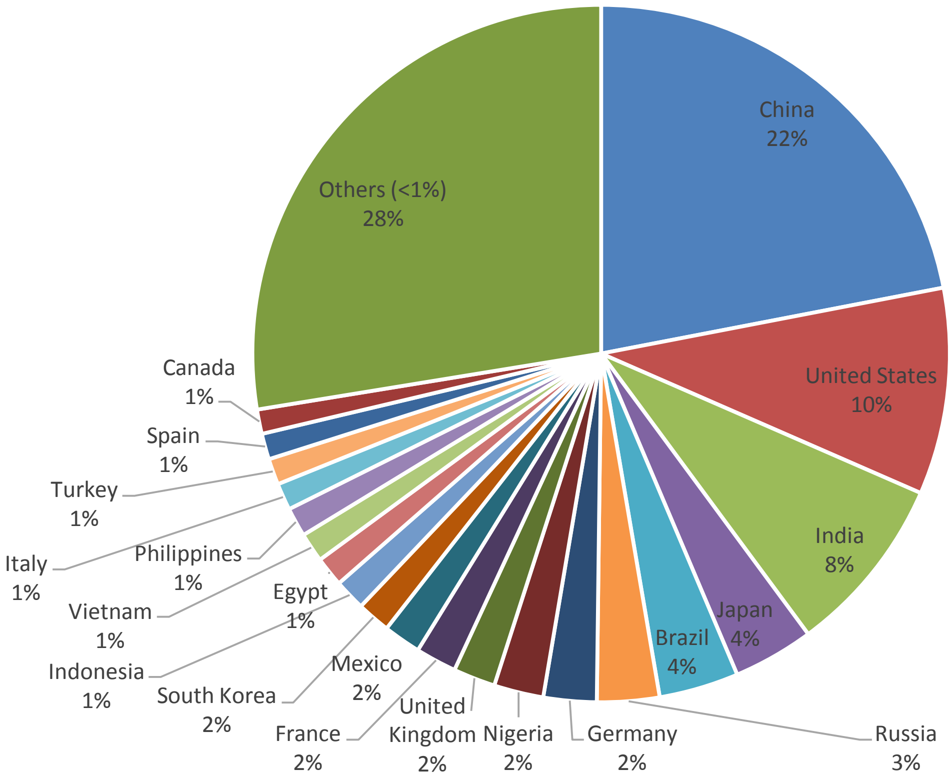
The metric will search for a relation between the average wealth and the average amount of attacks per inhabitant. Expected is that higher average GDP per capita will attract a higher amount of attacks per inhabitant.

## 5. Evaluation of the derived metrics

1. *"Uptime of phishing website per targeted country"*
   As mentioned earlier, the uptime data from Clean-mx differed from the XML-download and the data visible on the screen, resulting in very different usability than expected. Different from the XML-download, the screen-data contained at most 1 item per country except for the US. On a 1000 downloads, about 42 items belonged to other countries, and the rest was either blank or belonged to the US. A meaningful interpretation of the average uptime per country was therefore unfeasible. Instead, it was tried to fit a distribution to the data on US uptimes. A normal or Poisson distribution was expected. Highly surprising is that almost all uptimes are either 24 hours (over 10%) or around 10.000 hours (over 15%) and the rest is very scattered, making a distribution impossible. There seems no logical explanation for this.

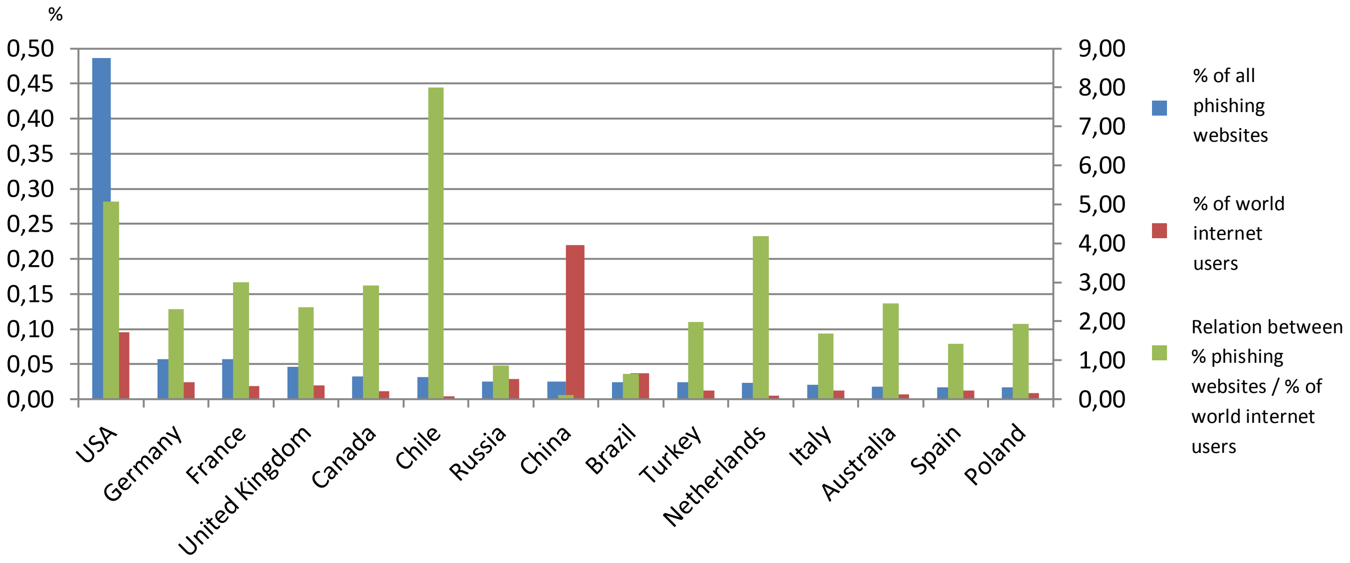
2. *"Number of internet users per targeted country"*
   These numbers were calculated according to the definition. The pie chart below shows what a country's share is of all internet users in the world. In this chart it is visible that not the USA, but China is the leader in this area, which is surprising given the attack statistics in which the US is targeted most.

Graph. Country's share of world internet users



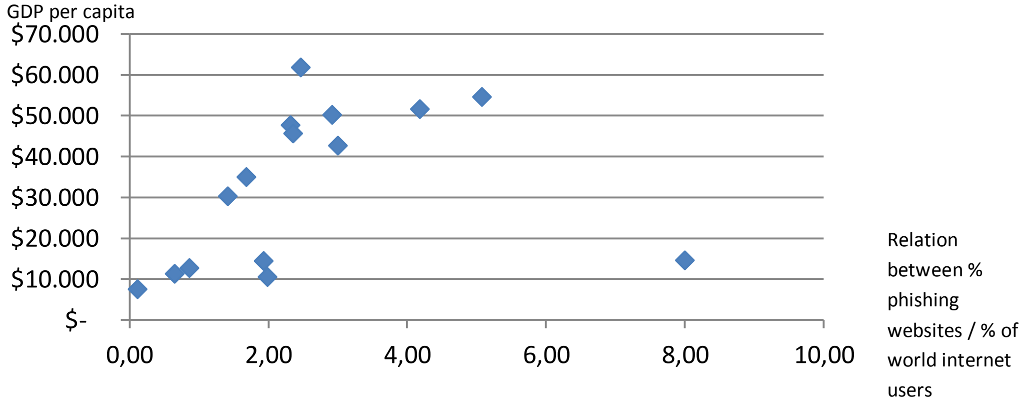
3. *"Number of attacks per country/region, normalised by the number of local internet users"*
   For the top 15 countries who have the most attacks, the share of phishing websites is compared to their share of the world's internet users. The blue bars represent the % of phishing websites that is aimed at the country. The red bars represent the % of internet users that live in the country. The green bars are the result of comparing the percentages to each other by dividing the % of phishing websites per country by the % of internet users in the country. This results in a number. The higher the number, the more attacks are aimed at each internet user in that country. Clearly Chile is targeted most – or Chile notifies the most phishing websites. Surprisingly, the Netherlands has almost the same rate of attacks per internet user as the US.
   Obviously it is not ideal to work with percentages only, because it gives no insight in the actual amount. However this is the best that can be derived from the available phishing data.

Graph. Percentages of world's phishing websites and internet users per country, and the relation between the two.



4. *"GDP per targeted country and presence of normalised targeted phishing"*
   The graph below shows the relation between the previously calculated metric – the relation between the % of the world's phishing sites in a country, compared to the % of the world's internet users in that country – and the GDP per capita in the country. Again, the graph shows an example for the same top 15 attacked countries. There does seem to be a positive correlation between GDP and normalised phishing attacks, although there is one outlier (Chile).
   However, GDP is known to correlate with a lot of variables. The actual value of this metric might therefore not be very high. Also the amount of items in this example is too low to interpret in a meaningful way.

Graph. Relation between GDP and normalised targeted phishing



## 6. References

- APWG (2013). *APWG Phishing Activities trend report 2013Q2.* Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf on September 17, 2015.
- Böhme, R. (2010) *Security Metrics and Security Investment Models*. International Computer Science Institute, Berkeley, California, USA
  Retrieved from:
  https://www.is.unimuenster.de/security/publications/Boehme2010_SecurityInvestment-IWSEC.pdf
- Chapin, D.A. & Akridge, S. (2005). *How Can Security Be Measured?* Publication by the Information Systems Audit and Control Association, retrieved from http://www.isaca.org/Journal/archives/2005/Volume-2/Documents/jpdf052-how-can-security.pdf
- Clean-mx (2014). *Phishingsite distribution top 25, 2014.* Retrieved from http://support.clean-mx.de/clean-mx/phishstats on September 25, 2015
- Clean-mx (2015). *Phish Stats.* Retrieved on September 15 via http://support.clean-mx.de/clean-mx/phishstats
- Clayton, R. and Moore, T. (2007). Examining the impact of website take-down on phishing. *e-Crime '07, Proceedings of the ant-phishing working groups, 2007, New York, USA.*
- DeBarr, D., Ramanathan, V., & Wechsler, H. (2013). Phishing Detection Using Traffic Behaviour, Spectral Clustering, and Random Forests. *Proceedings of ISI 2013, June 4-7, 2013, Seattle, Washington, USA.*
- Doshi, Provos & Chew (2006). A Framework for Detection and Measurement of Phishing Attacks. *A publication of the Johns Hopkins University Security Privacy Applied Research (SPAR) Lab. Technical Report SPAR-JHU:SD-NP-MC-AR:251206.*
- Gartner (2007). *Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks.* Press release, December 17, 2007, Stamford, Connecticut, USA. Retrieved from: http://www.gartner.com/newsroom/id/565125
- International Monetary Fund (2015). *World Economic Outlook Database, April 2015.* Retrieved from http://www.imf.org/external/pubs/ft/weo/2015/01/weodata/index.aspx on September 22, 2015. Choose “by countries”; “all countries”; “Gross domestic product, current prices (U.S. Dollars)”.
- Jaquith, A. (2007). *Security Metrics. The Definitive Guide to Quantifying, Classifying, and Measuring Enterprise IT Security Operations.* Unknown: Pearson Education.
- Miyamoto, D., Hazeyama, H. & Kadobayashi, Y. (2008). An Evaluation of Machine Learning-based Methods for Detection of Phishing Sites. *In: Proceedings of the 15th International Conference on Advances in Neuro-Information Processing, vol. 1, pp.539-546. Springer, Heidelberg (2009).*
- PhishTank.com (2015). *Stats*. Retrieved on September 15 via http://www.phishtank.com/stats.php
- The World Bank (2014). *GDP per capita (current US$) 2010-2014*. Retrieved from http://data.worldbank.org/indicator/NY.GDP.PCAP.CD on September 22, 2015.
- United Nations Statistics Division (2013). *National Accounts Main Aggregates Database, December 2013*. Retrieved from http://unstats.un.org/unsd/snaama/selbasicFast.asp on September 22, 2015. Choose “all countries”; "GDP, Per Capita GDP - US Dollars"; “2013”.
- Wardman, B. (2014). New tackle to catch a phisher. *Int. J. Electronic Security and Digital Forensics, Vol. 6, No. 1, 2014*

## Appendix A. Ideal metrics derived from brainstorm and literature

| **Metric** | **Explanation** | **Feasible or not** | **If not feasible, why?** |
|---|---|---|---|
| **On phishing websites – prevalence & effect** | | | |
| **Uptime of phishing website per targeted country** | Shows for how long the website has been online differentiating from country to country. It could be useful to analyse the suppression response of the various countries in order to evaluate their law enforcement. | Feasible. | |
| **Uptime of phishing website per business sector targeted** | Shows for how long the website has been online differentiating from country to country. Useful to see which sector pushes more for suppression. | Feasible, though hard. | |
| **Amount of phishing websites per business sector** | Shows which sector is more/less targeted. | Feasible, though hard. | Targets should be categorized and clustered in business sectors manually, this would lead to some (still incomplete) information |
| **Amount of phishing websites per business sector per country** | Shows whether in different countries different sectors are targeted more/less. | Feasible if metric above is determined. | |
| **Effectiveness of phishing website during time** | Meaning: what's the trend (if there is one) in the number of people filling in the phishing websites with valuable information?<br>We calculate effectiveness as the number of victims divided by the total number of visitors of the page. | Feasible. Reference: Moore & Clayton, 2007. | |
| **Money lost per incident / country / target / time** | Shows the amount of money lost due to phishing in the various dimensions. | Feasible/ unfeasible. Reference: "Measuring the cost of cybercrime", 3.2 online banking fraud | It's hard to determine the exact amount of money lost per incident. In some case the loss could be indirect. Also not every data is available. It has been estimated. |
| **Per country – Prevalence & distribution** | | | |
| **Number of internet users per targeted/origin country** | Useful to give a proper weight to country-based metrics. | Feasible. | |

| **Metric** | **Explanation** | **Feasible or not** | **If not feasible, why?** |
|---|---|---|---|
| **GDP per targeted/origin country and presence of normalised targeted phishing** | It could be interesting to study whether there is a correlation between a country's wealth and attacks. | Feasible. | |
| **Number of attacks per country/region, normalised by the number of local internet users** | Shows where phishing (as origin and targeted country) happens more/less.<br>The metric should be normalised accordingly to the number of internet users of that country/region. | Feasible. | |
| **Distribution of attack goals: identity theft, money laundering, espionage etc.** | Shows which goal is more less/popular in phishing attacks. | Not feasible. | Not all information is available.<br>Also multiple goals can be pursued with a single attack. |
| **Distribution of attack goals per country (both as origin or target)** | Shows whether different countries have different phishing problems. E.g. countries with more modern economy could suffer more from home banking phishing rather than other kind of phishing. | Not feasible. | Not all information is available.<br>Also multiple goals can be pursued with a single attack. |
| **Phishing e-mails – prevalence and effect** | | | |
| **Acceptance ratio of phishing emails through spam filters per e-mail client.** | It would be useful to study how many phishing emails are blocked by the various e-mail clients (Gmail, Yahoo!, Hotmail etc.), in order to understand which one is better. | Partly feasible. | Data on how many emails are stopped by filters should be obtained in collaboration with e-mail providers. However, there are both false negatives and false positives which make the metric less reliable. |
| **Acceptance ratio of phishing e-mails sent per criminal organisation (origin)** | Shows how many of the phishing e-mails sent by a certain criminal organisation arrive to the potential victims. Maybe some organisations have different ratios of acceptance. | Not feasible. | It's hard to have exact data related to specific criminal organisations. |
| **Average success rate per phishing email** | Success rate: how many people fill in real data after receiving a certain mail out of how many people receive the emails | Not feasible. | People can have more email addresses and keeping track of every single mail is quite hard. We could get an idea from surveys though this is not precise enough for the ideal metric. Data will be available at the criminal side, but this is not accessible for obvious reasons. |

| **Metric** | **Explanation** | **Feasible or not** | **If not feasible, why?** |
|---|---|---|---|
| **Number of phishing emails received pro capita per country, per time unit** | Shows how many emails a person receives on average per specific country in a determined period of time (a day, a week, a month, a year etc.). | Feasible, using for example data from ISPs and mail providers | |
| **Criminal perspective** | | | |
| **Revenue per criminal organisation related to phishing activities.** | Shows the profit of every single organisation gets from phishing related activities. | Not feasible. | It's hard to have exact data related to specific criminal organisations. |
| **Amount of phishing sites per criminal organisation.** | Shows how many online phishing websites an organisation has at a certain moment. | Not feasible. | It's hard to have exact data related to specific criminal organisations. |
| **Amount of criminal phishing organisations per country.** | Shows how many criminal organisations related to phishing exist in different countries. This value is useful both normalised to the number of Internet users of that country (or even the general population) and not normalised. | Not feasible. | It's hard to have exact data related to specific criminal organisations. |
| **Other** | | | |
| **Distribution of the lifespan of phishing websites during the days of the week** | Shows whether the speed of taking down a phishing website depends on the day of the week it is reported, e.g. if the takedown is slower on the weekend. | Feasible.<br>Reference: Moore & Clayton, 2007 | |
| **Number of attacks per specific target** | Shows which company is targeted more. | Feasible. | |
| **Number and distribution of mules per country, normalised by the numbers of local internet users** | Shows how many mules are present in the country. This metric should be normalised accordingly to the number of internet users of that country/region. | Not feasible. | The exact number of mules is really hard to measure. Data are scarce. It could be estimated. |

## Appendix B. Calculation and explanation GDP

GDP is short for Gross Domestic Product, which reflects the total amount of money made by a country as a whole. A large GDP does not necessarily point to a wealthy economic state; this can also be caused by a large number of workers inhabiting the country, or by a large amount of land available for production. In order to get an understanding of the wealth of a country's inhabitants – and thus their attractiveness to phishers – the GDP should be divided by the number of inhabitants, resulting in GDP per capita.

It is specifically chosen to use GDP *nominal* per capita, not *purchase power parity (PPP)*, since the metric should be able to compare between countries. GDP nominal per capita reflects the absolute level of wealth (in this case, in current US$), and is thus comparable to other countries. GDP PPP per capita reflects the GDP per capita in relation to e.g. the costs of living in a country, which shows whether the absolute GDP per capita actually results in a good standard of living within the country. This is not of interest to this study.

The data on GDP nominal per capita was retrieved from The World Bank (2014). When checked against other prominent databases, such as the International Monetary Fund (2015) and the United Nations Statistics Division (2013), no obvious dissimilarities are noted. Therefore it is decided to simply use the data from The World Bank.