Economics of Security — Security investment and Management

Tycho Teesselink (s1560506)
Tariq Bontekoe (s1451278)
Æde Symen Hoekstra (s1479679)
Ramon Houtsma (s1245228)
Group 13 — Phishing

October 2018

1 Problem owner

According to Lean Six Sigma, the problem owner is the person functionally responsible for the process a team is trying to solve. In our case this would be the security consumers, i.e. the security decision makers. They interpret the results of the metrics and decide what action needs to be taken. More specifically, they are the organizations and TLDs being targeted by phishing attacks. Organizations that are the most likely to be frequently targeted, are the ones that handle personal data or online finances, because personal information is valuable and fraudulent transactions can be made when a user is compromised. This makes them an attractive target for attackers because of the quick return on investment. TLDs also act as security providers because they deliver IT services and have the power to take down phishing sites.

In order to have a clear and unambiguous scope, for this research we will only consider the organizations that are targeted by phishing as problem owners. The TLDs will be discussed, but only as part of the ”other actors” that have an influence on the security issue.

2 Relevant differences in performance

The time it takes until a known phishing site is taken down differs per targeted company. For some companies the average uptime is only a couple of days, whereas for others it is months. The variety in response time is enormous and could be rigorously improved for most companies. The evaluation of this metric can be seen in figure 1. In this graph, the average uptime of the phishing websites (in days) per company is plotted against the number of phishing websites for the company.

In this metric both the average uptime and the number of phishing sites are taken into account. This is important, since for example, a big company such as Paypal has a lot of phishing websites targeting them, but on average they are taken down in about a month. In contrast, a much smaller company such as the Bank of Alapaha has a very high average uptime but this not necessarily means that they are doing badly since they only have a few instances of phishing. Companies that are close to the axes are doing relatively well whereas companies that are closer to the diagonal are doing relatively worse.

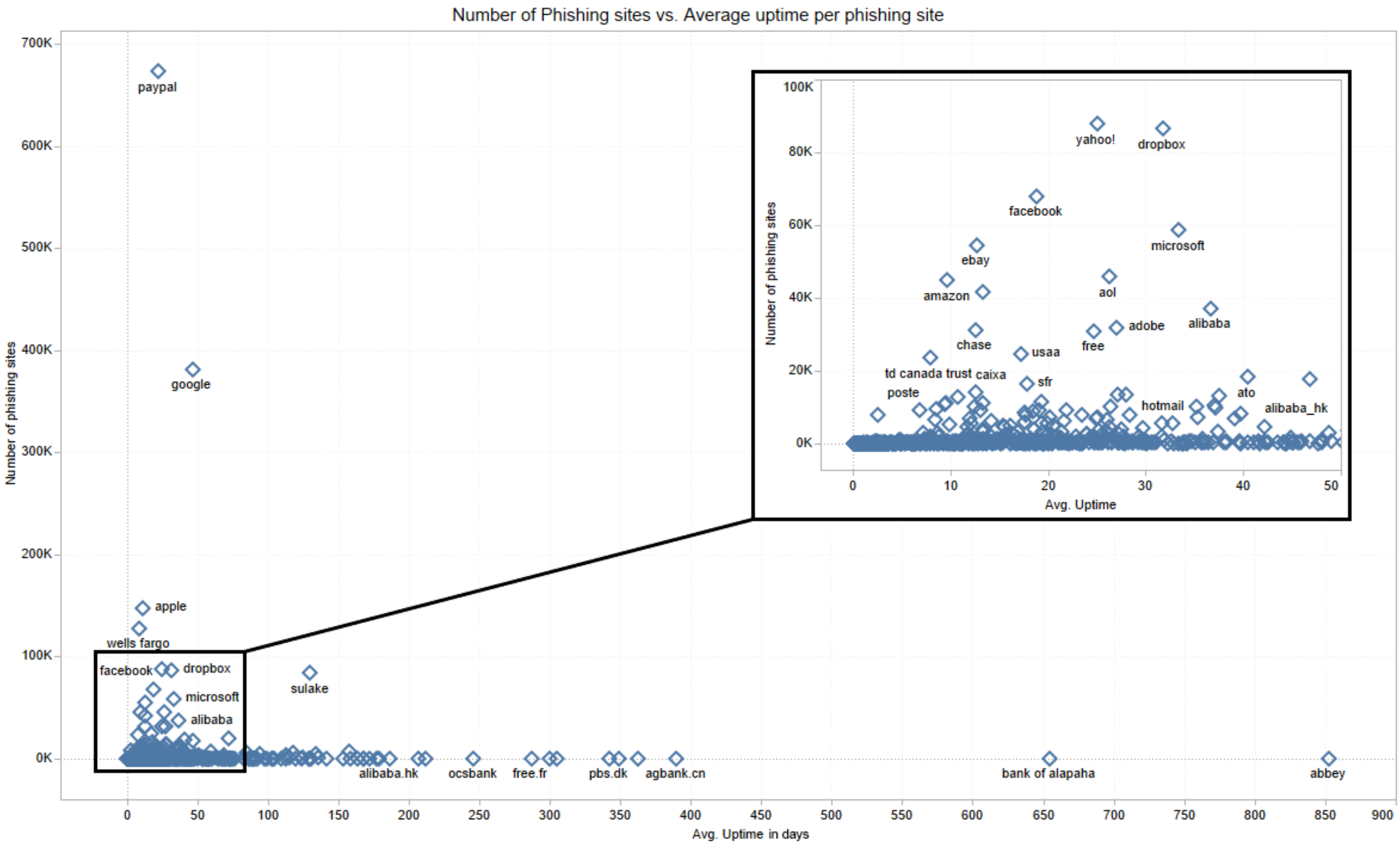

Figure 1: Number of phising sites vs. average uptime per phishing site

3 Risk strategies for problem owner

The organizations that provide online services are the security consumers. The security issue of phishing has direct impact on their business because it is their clients that are being targeted. The clients will be dissatisfied and may need to be compensated. We discuss four instruments in risk management to approach this security issue.

3.1 Risk mitigation

An incident response protocol is a series of actions that are executed upon materialization of a threat, in this case phishing. In this protocol actions that need to be executed will help in minimizing 'damage' caused by the threat. In this case, for example, taking down a website as fast as possible. By taking down the phishing websites faster, the risk of users falling for phishing is lower. Besides taking down the phishing websites, notifications can be sent to all users of the company's service, for example Paypal, that phishing websites are being used, and to pay extra caution when using their service.

Another mitigation strategy can be registering domains that are **similar** to the domain name of the organization, purely to prevent others from using these domains for phishing attacks. If these domains are unavailable for the attackers, the probability of people being phished may be lower and therefore the risk would be lower.

Using a smart intelligent phishing detection system to scan new websites is also a strategy. This early detection method to find phishing websites before they get used, in combination with the above mentioned incident response protocol, might greatly lower the risks. An example of such a system for e-banking is mentioned in a paper by Aburrous et al. [1]

It is also possible to hire a company that detects phishing websites and takes those websites offline as quickly as possible. [2, 3] This way companies do not have to bother with hiring professionals in-house in order to develop detection models, nor do they have to find out how they can take websites offline. However, in this case it might still be useful for companies to have an incident response protocol. The purpose of this protocol is to warn customers when the risk of being phished for this company is high.

3.2 Risk acceptance

When accepting the risks, the party accepts that incidents will happen. The losses and consequences will be reimbursed by the same party. For example, an e-banking provider will reimburse the losses due to fraudulent transactions on the consumer's account, if the account details were stolen by means of a phishing website. This strategy is usually only attractive when the costs (reimbursement, reputation damage etc.) are lower than the costs of other countermeasures. For example the remaining risk (along with the expected costs) after applying countermeasures does not outweigh the costs of an additional countermeasure.

3.3 Risk avoidance

Strategies to avoid the risks of phishing include withdrawing from or limiting online interactions. This is not a viable strategy for organizations with core online activities. For example Paypal cannot simply stop facilitating online payment transactions as this is their sole business model.

3.4 Risk transfer

Transferring risk means that another party is responsible for the consequences of an incident. An example of such a strategy is getting insurance. Since our example is phishing, the insurance party would reimburse any losses resulting from phishing and therefore the risk for the problem owners is transferred to the insurance companies. This type of insurance does already exist in practise, for example HDI has a program called Cyber+ Insurance [4], which covers losses caused by cyber crime and data breaches. Even though this takes away most of the liability for the initial party, this will most likely come with a hefty premium.

4 Other actors

Besides the problem owner, three other actors have been defined that can influence the security issue:

4.1 Website take-down companies

Website take-down companies are service providers of which the core business is taking down malicious websites in request of their customers. These companies charge a certain amount of money for every site taken down. Sometimes, they also provide services that actively monitor phishing and other malicious websites that are targeting their customers.

4.2 Hosting providers

Phishing websites are often hosted by hosting providers, instead the own servers of the phishers. Of course these hosting providers do not want to host phishing websites because of legal issues, as well as the problems phishing causes for their reputation. Hosting providers therefore benefit by banning malicious websites and cooperating in the take down of phishing sites that are brought to their attention.

Sometimes phishers make use of vulnerabilities in websites to serve phishing pages from the domain of some other website. Therefore it would also be beneficial for hosting providers to detect phishing sites that are unknowingly hosted by their customers.

4.3 Online service consumers

People are the weakest link in a system. In this case the system can be an online service. Even if the websites are super safe and have adequate security in place, if someone unknowingly provides their login credentials, all security is in vain. Therefore this actor also has a major influence on the security issue, for example by being, or not being educated on phishing.

5 Risk strategies for other actors

5.1 Strategies

5.1.1 Risk mitigation

Hosting providers can mitigate part of the risk by investing in a program that scans all pages served by customers and look for phishing pages. They can also prevent phishers from hosting by thoroughly verifying all customer info.
Online service consumers can benefit by educating themselves on, for example, the most common indicators of a phishing site. This can result in avoiding phishing sites more often, which will reduce the success of phishing campaigns.

5.1.2 Risk acceptance

Remaining risk that has not been mitigated by countermeasures can be accepted by hosting providers and registrars due to the fact that investing more money would yield very little to even negative returns on investment. This is however conditioned on the fact that certain laws, for example on privacy, are already being complied to by said mitigating measures.

5.1.3 Risk avoidance

Online service consumers may avoid the security risk by not using the online service. For example, they could go to the local bank to make payments instead of using online banking.

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

In the early days, when phishing was being used for the first time, not many people were a victim. This means that the losses caused by phishing were also low. Installing countermeasures were very expensive, and therefore it would be cheaper to accept the risk and reimburse any losses due to phishing. However, when criminals started doing large scale phishing campaigns, for example due to technological improvements, the losses increased immensely. This means that accepting the risks was no longer viable, and the strategy changed to mitigating the risk.

Another influencing fact here, is that technology became cheaper over the years. For example we have many machine learning methods that can help by identifying phishing websites, which makes it easier to decrease the uptime of a phishing website.
Because mitigating risks is usually only viable as long as the costs do not exceed 37% [5], by decreasing the costs, we can increase the amount of risk mitigated. Therefore, over time, the fact that the price of technology decreases lowers the risk. If the price of a mitigating measure exceeded the costs of accepting it, it was better to accept the risk at that time compared to mitigating it. If the costs are lowered, this could now be changed to mitigating risk.

6 ROSI calculation for risk transfer strategy

In this section we will calculate the Return on Security Investment (ROSI) of hiring a company that takes down phishing websites for you, a so called website-takedown service. We will perform this calculations for the company PayPal as it is often targeted by phishing attacks. It also has an average uptime that could still be somewhat improved but is not disastrously high. Usually, the ROSI is calculated with the following formula:

$$\text{ROSI} = \frac{ALE_0 - ALE_1 - c}{c}$$

In this formula the Annual Loss Expectancy without security measures in place is given by variable ALE_0 and the Annual Loss Expectancy with security measures in place is given by

ALE_1. The costs of the investment are given by c. This formula seems rather easy, however one has to take into account that the the variables are not simply discrete values. they are actually best described by a certain probability distribution. In the remainder of this section we will focus on obtaining the probability distributions of these variables, in order to get a final distribution for the ROSI.

We start by noting that the annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE), also called frequency or probability respectively impact. This can be mathematically expressed by the formula

$$ALE = ARO \cdot SLE$$

Please note that also here the values of ARO and SLE are probability distributions instead of discrete values.

From a research by Verizon [6] we know that approximately 4% of all people click on any given phishing campaign. As no data is present on the amount of people that get presented a specific phishing site, we have to make an assumption here. We assume that each day 1000 people receive a phishing email. Because this assumption is not based on factual data, resulting conclusions should be interpreted with caution. This means that each day approximately $1000 * 0.04 = 40$ people become the victim of phishing each day. Using the fact that a piece of stolen personal or confidential data costs approximately \$150 on average [7], we come to an expected amount of \$6000 per day of losses for a certain phishing site.

In Figure 2 the probability distributions of the impact and the probability without any security investment are depicted. Both distributions seem to be Poisson distributions, however the graph that shows the probability (Annual Frequency) has a really small second bar. This is probably due to the fact that the bar sizes are not optimal, however choosing a smaller or bigger bar size would result in a less explanatory graph so we have chosen to keep the bar size like this.

Using the distributions for the loss and the frequency, we arrived at a distribution for the Annual Loss Expectancy without security investment. This distribution can be seen in Figure 3. This distribution seems to be also Poisson, as to be expected, however this is a bit harder to determine due to the large fluctuations.

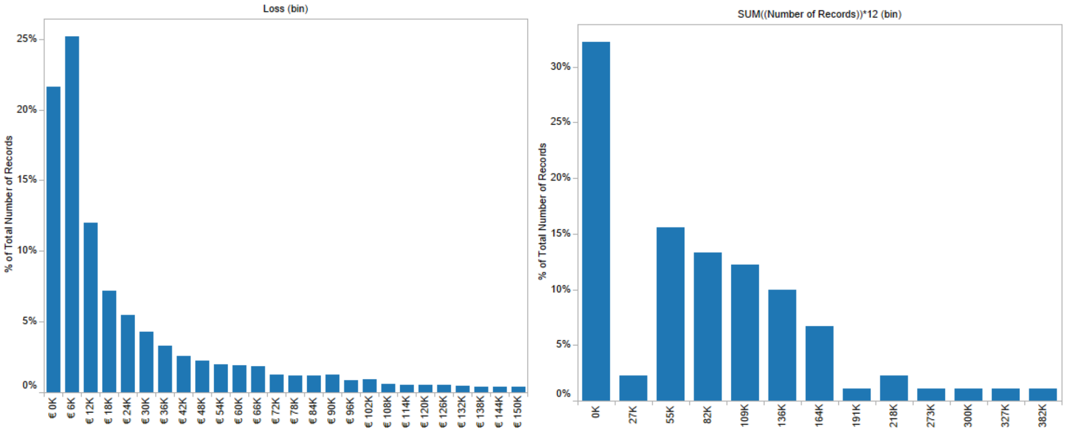

Figure 2: Probability distributions of Unitary Impact (left) and Annual Frequency (right) without security investment.

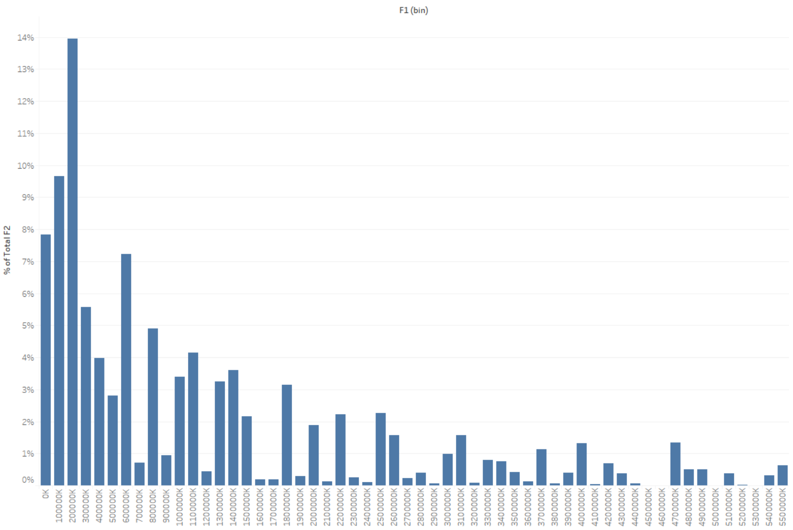

Figure 3: Probability distribution of the Annual Loss Expectancy without security investment.

With the security investment in a website-takedown service we expect the uptime to decrease in a way that the amount of phishing sites with a high uptime will decrease more than the amount of websites with a lower uptime. We approximate this by transforming all uptime values larger than 1 day. We take the power of its original uptime value to 0.75.

$$\text{New uptime} = \text{old uptime}^{0.75}$$

This seemed to be a sensible assumption which is somewhat based on the SLA of [8]. From the same service we also determined the costs of hiring such a service. From this source we concluded that a website-takedown service costs approximately $2000 (sunk costs) plus an additional $1000 (recurring costs) dollars per takedown. [8] The recurring costs as well as the changed uptime distribution lead to a new impact distribution which can be seen in Figure 4. We assume that the investment in a website-takedown service does not influence the annual frequency and hence keep the same distribution for this as can be seen in figure 2.

Combining the two distributions leads us to the distribution that can be seen in Figure 5, which represents the Annual Loss Expectancy with the security investment. Also this value seems to be Poisson distributed, again with high fluctuations.

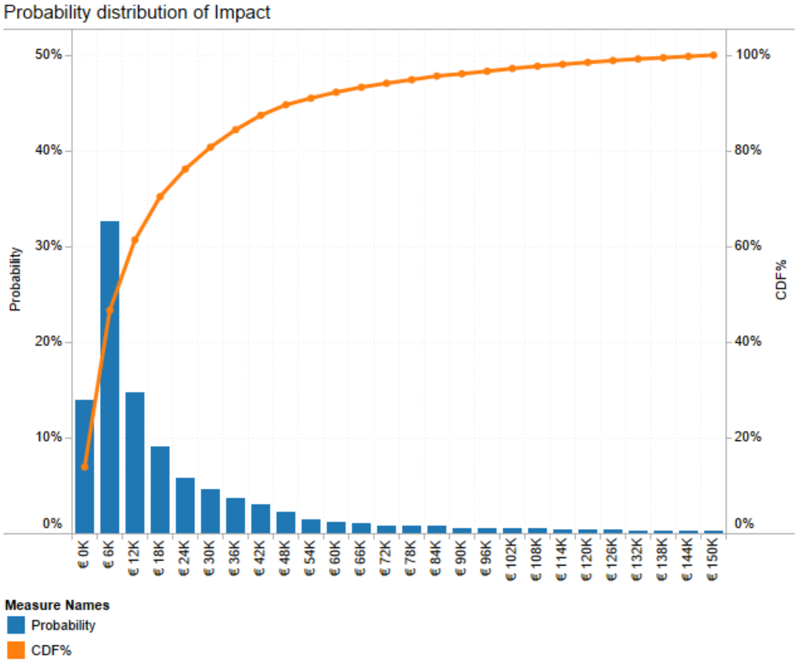

Figure 4: Probability distribution of Unitary Impact with security investment.

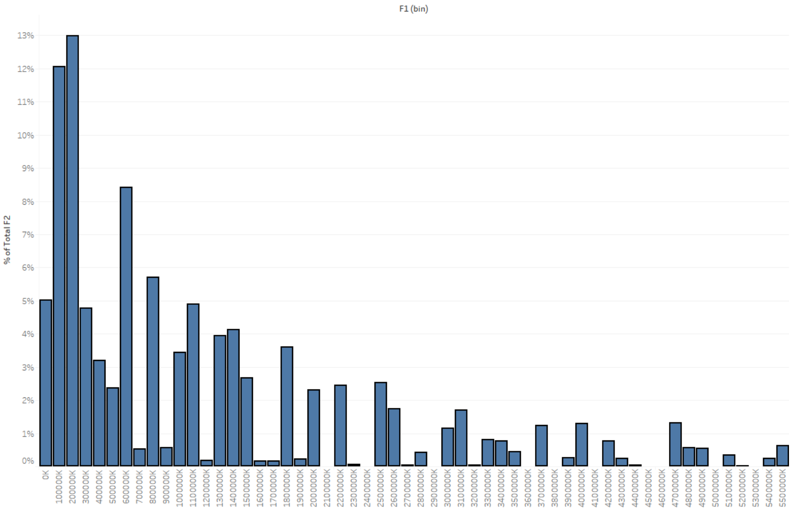

Figure 5: Probability distribution of the Annual Loss Expectancy with security investment.

Finally we will calculate the expected ROSI, as the fluctuations in our distribution were so high, that determining a distribution for the ROSI would give a non-sensible result. The expected ROSI value is determined using the expected ALE with and without the security investment and the sunk costs of $2000 for acquiring a contract with the website-takedown service. This value was approximately -115251% which means it is expected to be useless to make this investment. However, one can also see that our graphs containing the Annual Loss Expectancy's with and without the control have quite a large standard deviation. This is what makes it hard to pin the ROSI to an actual concrete value or even a ballpark, as the possible annual losses are so high.

7 Conclusion

The results of our study seem to be very pessimistic towards investing in website takedown services. The ROSI shows that investing in website takedown services is 115251 times not worth it. However because we made several assumptions we need to reflect a little bit on the results. To get a better view about what the actual ROSI would be multiple values should be considered for the losses per day for phishing. For example create the same graphs but for costs ranging from 4000 to 8000. Another possibility would be to check how much the costs should be to break even or even profit from this countermeasure. This again shows how hard it is to estimate accurately how much return on investment you can get from a security measure.

References

[1] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, “Intelligent phishing detection system for e-banking using fuzzy data mining,” *Expert Systems with Applications*, vol. 37, no. 12, pp. 7913–7921, Dec. 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417410003441

[2] “Fraudwatch international – anti-Phishing Protection Services & Solutions.” [Online]. Available: https://fraudwatchinternational.com/services/anti-phishing/

[3] “Sitetakedown – phishing Protection.” [Online]. Available: https://sitetakedown.com/services/phishing-protection/

[4] HDI, “Cyber+ insurance: covers losses caused by cybercrime and data breaches,” visisted on 26-09-2018. [Online]. Available: https://www.hdi.global/nl/en/insurance/cyber

[5] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, Nov. 2002. [Online]. Available: http://doi.acm.org/10.1145/581271.581274

[6] “Verizon 2018 data breach investigation report,” 2018. [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

[7] “IBM 2016 Cost of Data Breach Study - United States,” Apr. 2017. [Online]. Available: http://www.ibm.com/security/data-breach/

[8] “Sitetakedown – phishing Protection costs.” [Online]. Available: https://sitetakedown.com/products/