WM0824TU

Economics of Cyber Security

Block 3 Report - Group 13 - Phishing

Fiske Schijlen	(4947681)
Alexandros Korpas-Kamarianos	(4907167)
Joël Abrahams	(4443268)
Thanh-Dat Nguyen	(5025664)

{f.h.schijlen, a.korpas-kamarianos, j.s.abrahams, t.m.nguyen-3}
@student.tudelft.nl

October 6, 2019

Contents

1 Introduction **3**

2 Problem owner **3**

3 Differences in security performance **3**
3.1 Methodology 3
3.2 Results 4

4 Risk strategies to reduce the security issue **5**

5 Other actors who influence security issue **6**

6 Adoptable risk strategies **7**

7 ROSI calculation **9**
7.1 Estimation of risk exposure 10
7.2 Losses mitigated by the security controls 10
7.3 Cost of security controls 11
7.4 Final calculation 12

8 Conclusion **12**

1 Introduction

In the previous assignment, we have analysed a security issue and defined a set of metrics to estimate its impact. In this assignment, we are going to identify the actors that influence the security issue and determine what risk strategies should be used.

We first determine who the problem owner of the security issue is in section 2. We then outline differences in security performance found in the previously obtained metrics in section 3, after which we outline what risk strategies the problem owner needs to adopt to reduce the security issue in section 4. Next, we outline other actors who influence the security issue besides the problem owner in section 5. Following that, we outline the risk strategies that these other actors can adopt in section 6. Finally, we calculate the ROSI of one of the risk strategies in section 7.

2 Problem owner

Phishing attacks target a wide range of people. Most often, users are phished to gain their credentials to different services such as email or online banking. Not only are the users suffering from the ever so increasing phishing attacks, but also the organisations indirectly. Oftentimes, organisations have to deal with the consequences of the attacks on their users. Take the example of PayPal: Attackers, who have gained access to the user's account, can perform unauthorised withdrawals from the user's balance. PayPal reimburses the losses that fall on the users. The costs for PayPal are beyond reimbursing the transactions. PayPal incurs costs when investigating the unfortunate event and when tracing back the transactions. As such, we identify organisations as problem owners (as opposed to individuals).

3 Differences in security performance

It can be in an organisation's best interest to effectively counter phishing attacks to protect their users. To gain insight as to how effective organisations are, we can model the up-time of phishing websites impersonating organisations. One key assumption here is that the organisations themselves are the one taking down these phishing sites, and not some centralised entity or the hosts themselves.

3.1 Methodology

We model the up-time of the 5 most occurring virus names (virusname) over time. In other words, we group phishing domains by organisations they impersonate. We measure the up-time by subtracting the start date from the end date. For each organisation, the up-time is averaged per month.

We discard entries with no virus name in the dataset, because these entries don't provide any insight in this context.

3.2 Results

We plot the average up-time per month of phishing domains impersonating companies, which can be seen in figure 1.

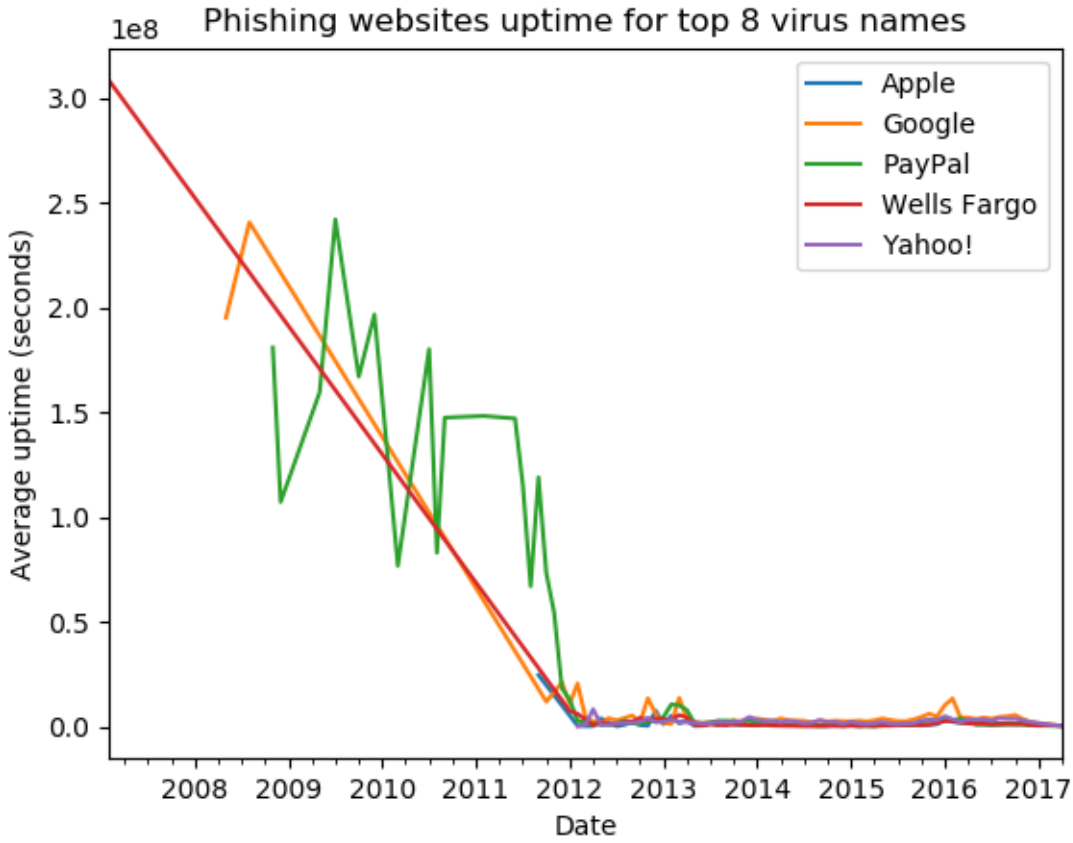

Figure 1: Up-time of top 5 companies in seconds

We notice that the up-time varies greatly between pre- and post-January 2012, with the data being very sparse and coarse before January 2012. We don't know the underlying reason for this disparity, though this might be attributed to the methods of collection used or simply errors made when congregating all the data points. As a result, we choose to focus on the up-time of the 5 most occurring virus names after January 2012. The resulting figure can be seen in figure 2.

Note that the up-time is displayed in the amount of seconds multiplied by $1e7$, or 10^7, so 1.0 seconds becomes 10000000 seconds, or roughly 115 days ($\approx$ 4 months).

We first note that there are large spikes at the end of 2012, till the start of 2013, and around the start of 2016, indicating that either a lot of phishing attacks were initiated around this time, or that it is easier to detect phishing attacks that are initiated around this time. Second, Google tends to have a higher average up-time than the other entries, with Yahoo! not falling far behind. Note that Google and Yahoo both provide email services. Furthermore, a clear spike at the start of 2013 for PayPal can be seen, though afterwards

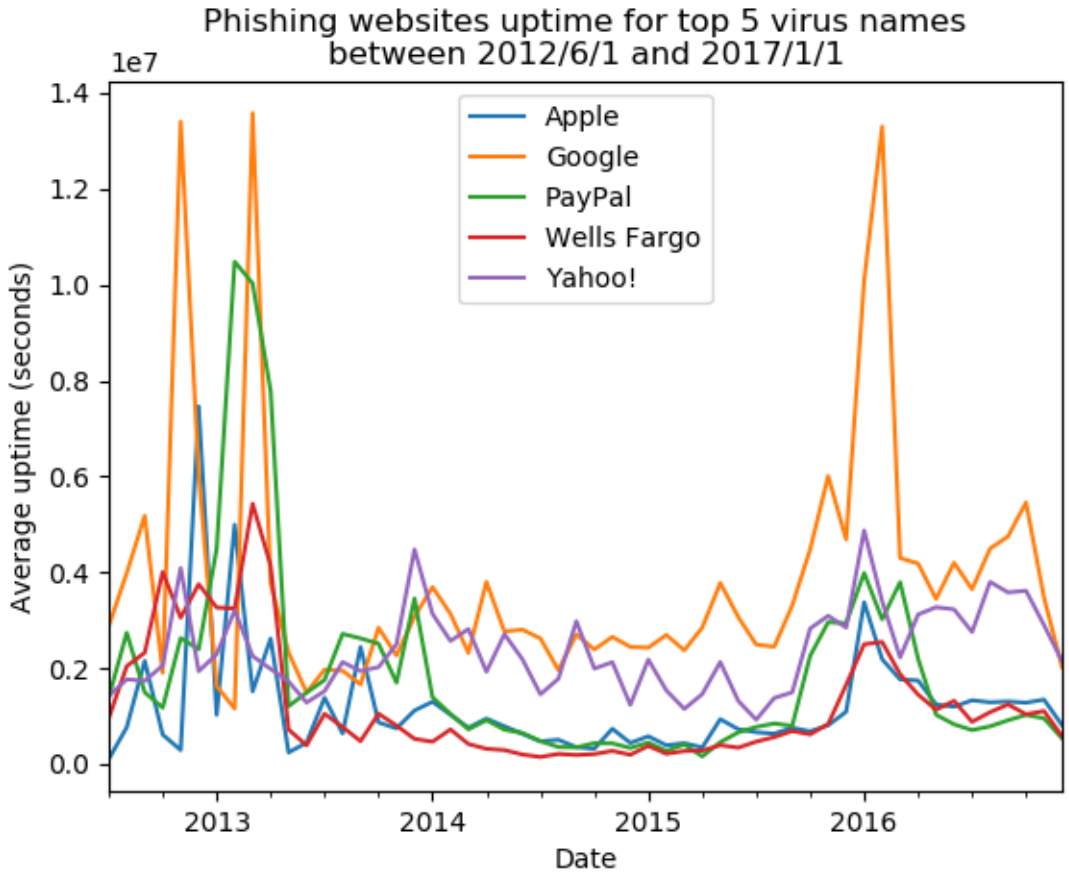

Figure 2: Up-time of top 5 companies in seconds from July 2012 till January 2017

there is a strong decreasing trend, as PayPal follows the general trend, with a smaller spike around 2016.

In general, the data seems to indicate that PayPal and Yahoo! show much improvement, whereas Google seems to be struggling with taking down phishing hosts as the spike in 2016 is near-identical in size to the 2013 one. This is also likely in small part due to the sheer amount of users of Google, likely meaning that there are more phishing websites due to this market being more attractive to phishers.

4 Risk strategies to reduce the security issue

There are four risk strategies that can be adopted by an organisation: mitigation, acceptance, avoidance and transfer. To reduce the security issue, however, organisations can only mitigate the risk involved. The other 3 allow an entity to deal with the security issue, but they do not improve the situation. The follow actions could be taken to effectuate *risk mitigation*:

- Take down phishing domains;

- Develop awareness programs for users and employees;
- Invest in phishing detection;
- Deploy stricter security policies.

5 Other actors who influence security issue

There are numerous actors that influence the security issue besides the problem owner. It is crucial to take all the actors into account to perform a proper risk analysis and determine appropriate risk strategies. Listing all the associated actors allows to provide a good overview of the security issue. In view of this, we list the most prominent actors below.

End-users

End-users are the biggest group targeted by phishing attacks. These attacks aim to steal credentials from users to impersonate them for various unauthorised activities such as withdrawing money from the victims bank account. Employees receive phishing emails and face the direct risk of giving the attacker confidential information if they do not correctly identify the email as malicious. By falling for phishing attacks, users are negatively impacting the security issue.

Employees

Next to the users, employees are also faced to phishing attacks, more specifically spear phishing. These attacks aim to steal the credentials of the employees, so that they can be used to access sensible data from the organisation. By falling for phishing attacks, employees are negatively impacting the security issue.

Cyber crime fighters

Cyber crime fighters are parties that either are an unit within the organisation or are a separate entity that take measures to improve security and mitigate attacks in regards to the organisation. They are authorised to detect, prevent, and respond to cyber crime, such as phishing. Such measures can be awareness programs for users and/or employees, taking down phishing domains, etc. Cyber crime fighters generally improve the security situation.

Security policy makers

Security policy makers are external bodies, such as governments, that create policies and regulations to improve the safety in the cyberspace. Organisations need to comply to those new set rules to be able to continue their business smoothly. In general, security policy makers positively influence the situation.

Security decision makers

Security decision makers are an unit within the organisation that takes financial decisions to deal with cybersecurity. Depending on their decisions, the security situation can improve or worsen.

Attackers

Attackers in this context are developing phishing attacks to exploit various organisation by impersonation. Attackers are the main cause of the security issue.

6 Adoptable risk strategies

The actors' strategies are based on the following four common risk management methods:

- Risk mitigation: reducing the likelihood and severity of loss events by protecting your assets.
- Risk acceptance: an organisation chooses to tolerate losses.
- Risk avoidance: the organisation withdraws from a risky business scenario.
- Risk transfer: a contractual agreement with a third party to compensate the organisation for losses incurred due to the realisation of risk.

End-users

End-users face the risk of losing important credentials in phishing attacks. These can be used to access accounts to do unauthorised activities such as withdrawing money or changing passwords. The compromise of one account can disrupt other services that they use. It is in their best interest to be safe from phishing attacks.

- Risk mitigation: usage of security software that includes protection from phishing emails; secure habit adoption (e.g. sender verification before opening the email or checking a URL before clicking on it), changing passwords regularly, using two factor authentication (when applicable);
- Risk acceptance: the end-user accepts the scenario of becoming a victim of a phishing attack;
- Risk avoidance: the end-user stops reading emails or services that put him in danger of getting phished;
- Risk transfer: buying an insurance or using a service that has phishing protection.

Employee

Employees, as end-users, are faced with the risk of revealing important credentials. The difference between employees and end-users is that the attacker can with the newly obtained credentials, damage the employee's reputation in his organisation and also in the industry sector. This can cost him his job and career.

- Risk mitigation: participating in employee awareness training, frequent changing of credentials, implementing automated phishing detection;
- Risk acceptance: accepting that authorisation credentials will periodically be lost due to successful phishing attempts, accepting the heightened risks of other attacks due to lost credentials;
- Risk avoidance: no longer reading emails even though this is highly impractical;
- Risk transfer: having a third party evaluate incoming emails to detect phishing attempts.

Cyber crime fighters

Cyber crime fighters face the risk of spending resources on anti-phishing measures that end up being ineffective. This lowers the fighters' reputation and results in them not being contracted for future anti-phishing campaigns.

- Risk mitigation: spending resources on the development and distribution of effective phishing detection methods;
- Risk acceptance: not spending time on phishing detection due to phishing's supposedly lower risk compared to other cyber crime or lack of rewards for the cyber crime fighters;
- Risk avoidance: stating that phishing is not on the cyber crime fighters' radar;
- Risk transfer: recruiting a third party, such as a software development company or other cyber crime fighters, to develop anti-phishing measures.

Security policy makers

The security issue does not directly affect them, but their incentives to design a risk strategy are driven from the nature of their role. Thus, acceptance, avoidance, and transfer of the risk are not applicable methods for them.

- Risk mitigation: create standards about protection from phishing attacks and oblige organisations to follow them.

Security decision makers

The security decision makers deal with the risk imposed on the organisation. They try to make the best financial decisions to deal with the risk.

- Risk mitigation: choosing the right security controls to implement to mitigate phishing threats;
- Risk acceptance: incurring phishing-related losses with the justification that phishing is not a large problem;
- Risk avoidance: stating that phishing is not on this party's radar;
- Risk transfer: having someone else make the decisions for them, with the promise of being reimbursed if the made decisions backfire.

Attackers

The risk of the attackers is different from the other actors as they only want to protect themselves from not getting caught.

- Risk mitigation: anonymity techniques;
- Risk acceptance: getting caught is always a possibility;
- Risk avoidance: careful selection of the targets;
- Risk transfer: not applicable to attackers.

7 ROSI calculation

We previously identified the end-user as a significant actor regarding our security issue. Whenever an end-user becomes a victim of a phishing attack, the company has a number of direct or indirect losses, as it is often so that end-users are protected with an insurance policy or because their reputation is damaged. Hence, in this section, we will present a mitigation strategy of that a company could follow to reduce the risk of the security issue. This strategy consists of the following steps:

- Launch a campaign to increase users' awareness of phishing attacks;
- Implement a 2-factor authentication policy.

Then we will compute the Return of Security Investment (ROSI) in order to assess the aforementioned mitigation strategy. To calculate ROSI, we will use the following formula:

$$ROSI = \frac{RiskExposure * \%MitigatedRisk - InvestmentCost}{InvestmentCost} \tag{1}$$

where the names of each variable are self-explanatory.

We will compute the *Risk Exposure* as the unitary impact multiplied by the annual amount of successful attacks, where the former will be defined through research and the latter using the provided dataset. However, our dataset doesn't provide any information regarding the success of the recorded attack. Thus, we will make an estimation of the total phishing attempts and we will multiply it with a success factor that will be determined through research. Furthermore, we will define the *Mitigated Risk* by making some assumptions about the effectiveness of our proposed strategy. Finally, we will define *Investment Cost* by using market research to determine the costs of the steps of our mitigation strategy.

7.1 Estimation of risk exposure

According to Litan [1], the average cost of a successful phishing attempt is 900 dollars. Since there is no official data on the deviation of these costs, we will assume the corresponding normal distribution has mean $\mu = 900$ and $\sigma = 0.1$, meaning the cost falls in the range [810, 990].

In 2019, Gordon, G. et al found that the median click rate for phishing emails directed at US health care employees was 16.7%.[2] Due to the lack of information regarding general phishing success rates, we will use this percentage as a success rate for general phishing attempts for this assignment's purposes.

Using our dataset, we determined that an upcoming year is likely to have about 2159052 occurrences, which means it is likely to contain $0.167 * 2159052 \approx 360562$ *successful* attempts. Then the occurrences would fall in the range [324506, 396618].

We combine the frequency and impact distributions to find that **the incurred costs will be in the range [810*324506, 990*396618] = [262849860, 392651820]**. We can then represent this range with a normal distribution with mean $\mu = 327750840$ and $\sigma = 0.1$. This distribution represents the probabilities of $RiskExposure$ having certain values.

7.2 Losses mitigated by the security controls

The mentioned security controls are designed to decrease the *effectiveness* of phishing attacks, but they will not affect the total amount of attacks.

- **Awareness campaign**: The effectiveness of this security control can vary between different organisations' user bases. If we assume its effectiveness to be equal to the effectiveness such a control would have on employees, we can define this control to mitigate a phishing attack's success rate by up to 15 percent.[3]

- **2-Factor authentication policy**: With this policy, we expect phishing attacks to become significantly more difficult to execute. This is because the attacker will have to obtain some sort of one-time password along with a user's other credentials. Though there are no specific mitigation statistics for this control, we assume that this policy is at least 50 percent effective in mitigating phishing attacks.

When combined, the controls reduce the phishing attacks' effectiveness to $0.85 * 0.5 = 0.425$, which means that $MitigatedRisk = 0.575$.

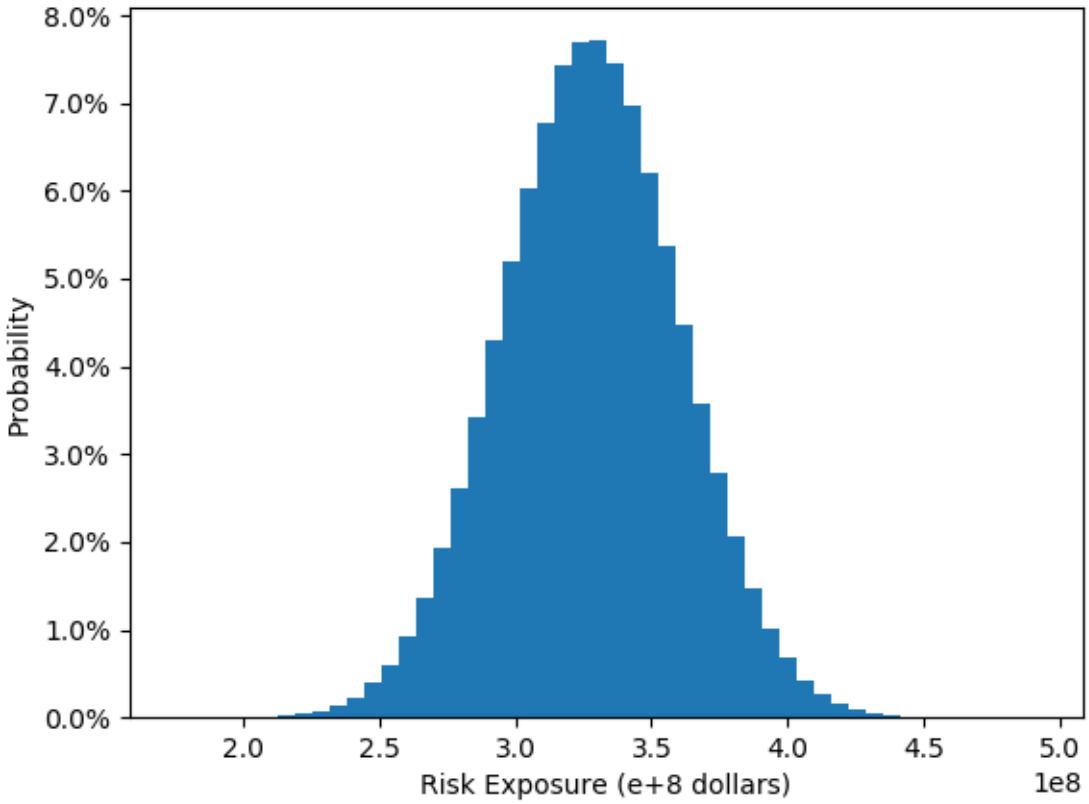

Figure 3: Distribution of Risk Exposure in dollars

7.3 Cost of security controls

To define a value for c, we need to define the respective costs of our proposed security controls.

- **Awareness campaign**: Launching an awareness campaign for its users requires the organisation to (1) recognise and define common phishing patterns, (2) clearly describe why phishing is a risk for users, and (3) communicate this information to the users.

  The costs and exact actions for steps 1 and 2 vary per organisation; smaller and larger companies will have differing amounts of yearly phishing threats and organisations that store more sensitive user data create more risk for the users. Larger organisations may also want to execute step 3 using a web page or other communication channels besides email, which would end up costing a lot more.

  A small organisation that faces a small amount of phishing threats and has a simple phishing risk definition for its users can send some awareness emails and leave the cost at about 200 dollars. An extremely large organisation with a complex risk definition may have to assign a small team to a campaign that informs its users through multiple platforms instead of just emails. Recognising patterns and describing a complex risk

will require a more specialised team that might have to spend a month to fully construct such a campaign. Assuming this could require a 4-man team that gets paid up to 40 dollars an hour, such a campaign could cost up to 25600 dollars. Since phishing awareness campaigns have significantly more merit for larger organisations that deal with users' financial data, we assume the cost of this security control to be **25600 dollars**.

- **2-factor authentication policy**: Adopting such a policy requires the organisation to change the back-end server that handles the users' credentials. Thus, the organisation need to hire a developing team or a third-party company that will formulate the software requirements and architecture of the new server, implement it, and migrate the new service to the existing infrastructures of the company.

  The costs of the aforementioned policy can be different accordingly to the number and the complexity of the software requirements. However, a reasonable assumption is to say that a development team of 6 people that is paid with 40 dollars per hour needs about 6 months to complete the implementation of the project. Hence, we can assume that the cost of this security control is **230400 dollars**.

  Furthermore, a consequence of this choice might be that some users will prefer to change to another organisation that provides a similar service, since they find this policy inconvenient. Thus, the new policy's costs of the organisation might be increased because of losing some clients. However, these losses are hard to be estimated, since they depend on multiple factors, such as the availability and the quality of a similar service, the commitment of the end-users with the organisation, etc. Thus, this cost factor will not be taken into account.

These estimations add up to a total of $InvestmentCost = 256000$ dollars.

7.4 Final calculation

Using a probability density function based on our estimation of annual risk exposure and the formula of ROSI (see equation 1), we can construct a bell curve that describes the distribution of the ROSI.

As it is clearly visible on the figure 4, the proposed strategy presents a mean value of $ROSI = 800$ which means that the proposed investment will provide significantly high benefits compared to the total cost of the investment.

8 Conclusion

We have determined that organisations who store user account information are the primary problem owners regarding phishing threats, because they often have to compensate users for their losses, deal with reputation damage, and face increased probabilities of more significant threats due to lost employee credentials.

Using *monthly average phishing threat up-time* as a metric, we compared several organisations' security performance over the years. We found that the top 5 most targeted

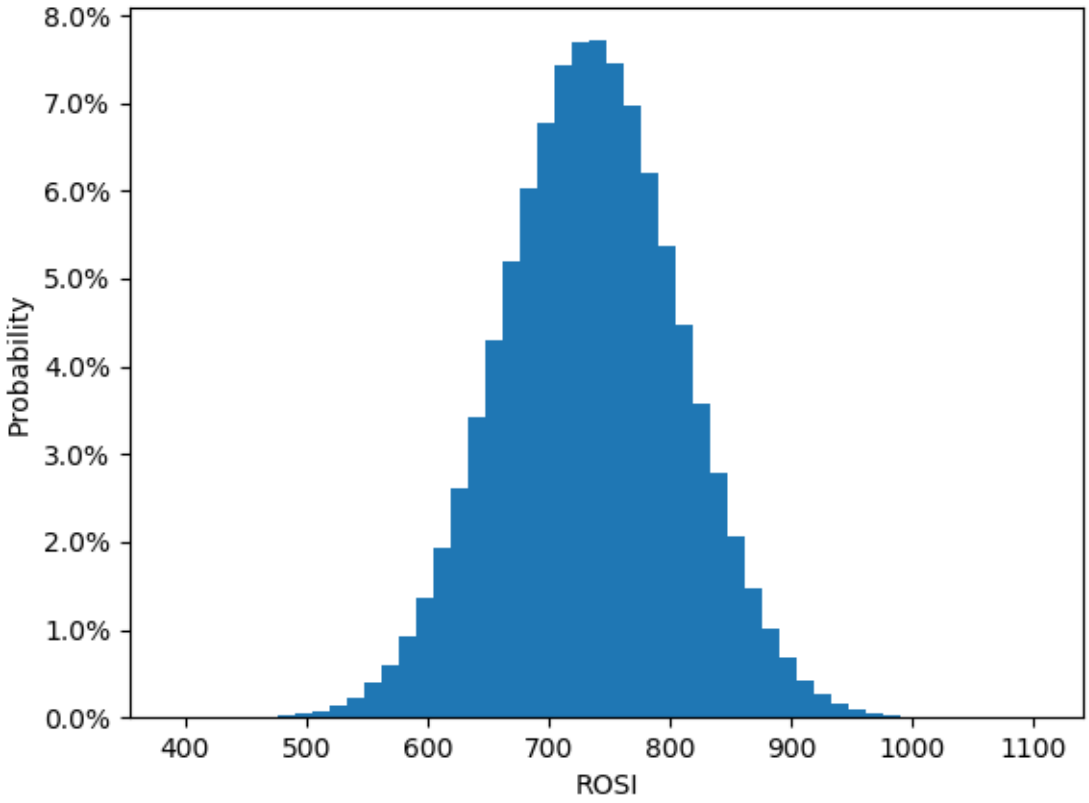

Figure 4: Distribution of ROSI for the proposed strategy

organisations from our dataset in general faced decreased threat up-times over the years until from 2013 onward, with a spike occurring at the start of 2016 after which the decreasing trend continues.

Furthermore, we identified end-users, employees, cyber crime fighters, security policy makers, security decision makers, and attackers as actors who could affect the effectiveness of phishing threats in one way or another. We identified organisations, end-users, and employees as actors with an especially large amount of options for risk strategies, though all of the aforementioned actors at least have the option a mitigation strategy.

Finally, we used our dataset and publicly available phishing research to calculate the *ROSI* for an organisation's risk mitigation strategy. This mitigation strategy involved launching an awareness campaign for end-users and implementing a 2-factor authentication policy to reduce the success rate of phishing attempts. Using our calculations and a set of research-based assumptions, we constructed a ROSI distribution that indicated the mitigation strategy would definitely be worth implementing.

References

[1] A. Litan, "Phishing attack victims likely targets for identity theft," 2004.

[2] W. Gordon, A. Wright, R. Aiyagari, L. Corbo, R. Glynn, J. Kadakia, J. Kufahl, C. Mazzone, J. Noga, M. Parkulo, B. Sanford, P. Scheib, and A. Landman, "Assessment of employee susceptibility to phishing attacks at us health care institutions," *JAMA Network Open*, vol. 2, p. e190393, 03 2019.

[3] I. Dimov. (2019) Security awareness statistics. [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-awareness-fundamentals/security-awareness-statistics/