WM0824 Economics of Cyber Security
Assignment 3

Maria Simidžioski	Sam van Hooff	Tom Slooff
4381319	4247620	4492919

October 2019

1 Introduction

The problem owners play a major role in the implementation of security strategies and mitigation of potential incidents with regards to website defacement. We will identify and discuss several actors that have a direct influence on the security level of the Autonomous Systems. The actors that are chosen are the AS administrator, the website owners and the regulatory authorities.

Assessing the distribution of costs and benefits in this environment helps in identifying why certain mitigation options are not pursued by actors. Especially for governmental bodies it is useful to identify externalities which are stopping actors from pursuing mitigations beneficial for society. Then if it is possible there may be incentives put in place such that these mitigations are pursued, and society can benefit from them. This may be more effective than regulation.

Lastly the effects of external factors on security metrics is investigated. This helps actors in assessing their own security performance. By investigating external factors the actors can identify the most important factors, and assess which ones they can control and which are out of their control. In this way the actors can develop an effective security strategy to improve their security performance.

2 Actors

In this section, three actors involved in the security problem are discussed. In each subsection, a counter measure for this actor is proposed, the costs and benefits are analyzed, and the incentive for this actor to take this counter measure is described. Lastly the externalities for this counter measure are described.

2.1 AS administrator

The AS administrator has the option to examine the configuration and basic security measures of the servers on its network. Most website defacements are the result of poor configuration of the server and could be easily avoided. By detecting vulnerable websites, and encouraging the website owners to fix their security, the AS administrator could cutback the amount of defacements on its network. This countermeasure would be easy to implement, however the effectivity is also dependent on the willingness of the website owners to act.

The costs for finding vulnerable websites lie entirely by the AS administrator, while the benefits are for the website owners as well as the AS administrator.

The benefits for the AS administrator mainly are a healthier network with less defaced websites and a better reputation as a result. This might result in more loyal customers and the attraction of new customers. Also possible fines for not handling website defacements properly might be avoided.

The benefits for the website owners is free advise about the security of their website, and how it might be improved. When a website owner gets a warning that its website is not properly secured, it can decide for itself if it wants to address the problem or not. In case it decides to act, the cost for improving the security of the website are for the website owner.

The AS administrator has an incentive to introduce the countermeasure discussed earlier, since it's goal is to achieve a higher level of security on its network. The costs for finding vulnerable websites on its network are probably quite low, since it is possible to automate this task. Even if only a small part of the alarmed website owners decide to fix the vulnerabilities on their website, the benefits for the AS administrator are substantial.

Externalities play a big role in this countermeasure. This is the case because the direct benefits of the countermeasure are mainly for the website owner, while the costs are for the AS administrator. The incentive for the AS administrator to implement this countermeasure anyway, is because of the indirect positive effects for the administrator when a website owner decides to improve its security.

2.2 Website owners

Website owners have the option to penetration test their own website, which results in a more secure website. For this measure the website owners experience most of the benefits, and they also bear all the costs. Penetration testing is an effective way of securing your website, but it is also expensive. Through penetration testing the website owners may greatly reduce their amount of defacements. This is a benefit for the website owner, but also an external benefit, namely for the AS administrator. AS administrators may be tasked with dealing with website defacements by regulatory authorities, which mean costs for them. Additionally the AS administrator may get less fines for this, and may get a better reputation. However, on the scale of one website getting secured these benefits are practically non-existent. The AS administrators can also experience costs from the penetration test, depending on how it is executed. If the penetration test involves some automatic scanners, this may be a large load on the network which causes costs for the AS administrator, as their available bandwidth is tem-

porarily reduced. The regulatory authorities do not have any costs or benefits because of this counter measure.

The incentive for the website owner to deploy this counter measure depends on several factors. Important ones are the cost of the penetration test, and how effective it is at mitigating defacements. But for a company to consider this counter measure, characteristics of the company itself may be even more important. For example small companies will probably care less about this attack, as they are less likely to be targeted. If the company does not have a reputation which attracts activists, they may not consider website defacements as relevant. The costs in relation to the budget of this company may be too large. Additionally, the costs of website defacement for smaller companies are not as large as for big companies which have thousands of visitors every day. Thus the incentives depend largely on characteristic of the business and the business environment it operates in, in addition to the direct costs and benefits of the counter measure.

The previous paragraph described the incentives for the website owner to deploy the counter measure. The externalities involved in the counter measure were not mentioned, as these do not play a large role in this counter measure. This counter measure has some external benefits for the AS administrator, as mentioned in the first paragraph of this section, but these are effectively quite small. The majority of the benefits are enjoyed by the website owner itself, meaning that externalities do not deter the website owner from deploying this counter measure. There is one possibly relevant external cost for the AS administrator. If the penetration test is not carefully executed, this results in costs for the AS administrator in terms of lost bandwidth and network congestion. If the AS administrator notices this, this may come back to the website owner and give some costs. But this is most probably not the case, so the website owner may not care about it.

2.3 Regulatory authorities

Regulatory authorities could impose stricter regulations as a countermeasure for the security issue of website defacement. They could for instance design certain standards to which the industry needs to adhere. It highly depends on this design and on the decision on who is held liable, how the costs and benefits are

distributed. An option would be that the regulatory authorities introduce new laws, which force an AS administrator to maintain a certain security standard on its network. They could for example make a new law which states that the network an AS is governing may never contain more than x defaced websites. Or a law that defaced websites should be resolved within an hour. If an AS administrator fails to comply, the regulatory authority could impose a fine. Of course regulatory authorities could also choose to hold the website owners responsible for a defaced website, in which case the costs for fines are for the website owner instead of the AS administrators.

The costs of stricter regulation for the regulatory authorities is spread over several factors. Initially, passing the regulation may require a lot of hours of work and thereby a lot of costs. After the regulation is passed, the costs of enforcing this regulation compared to more loose regulation are also larger. The regulation needs to be enforced in order for it to have an effect, and stricter requirements also means stricter monitoring and thereby more costs.

The benefits for a regulatory authority are different than for any other actor, as they do not evaluate the strategies from the perspective of their own benefits. Directly the regulatory authority will not experience any benefits. A regulatory authority looks at the benefit of the society, and aims to improve the situation in society by means of regulation. In this case the benefits for the regulatory authority would be the level of security in ASs. The regulatory authority aims to improve this, and so this is the perspective from which a cost benefit analysis will be made. In this sense, the measures need not only result in benefits, the costs also need to be realistic for society. Implementing a regulation of taking down defaced websites in 5 minutes may result in more secure networks in theory, but in practice this might be an unrealistic expectation, and it will only result in fines and AS administrators going out of business. Thus the benefits for the regulatory authority will be the benefits (compared to the costs) for society with regards to this security issue.

It is difficult to asses the distribution of costs and benefits of regulation among different actors. Regulation often produces costs and benefits for a society as a whole (Renda et al. 2013). However, with this statement it is also clear that there are a lot of externalities with any security strategy chosen by the regulatory authorities. A lot of costs will go to the party which is liable for website

defacement, or the party which is responsible for adhering to certain standards. However, the benefits are also for these parties. The AS administrator may be tasked with quickly removing defaced websites, which incurs costs for them, but they also benefit from having a cleaner network. Thus the role of externalities in these security strategies is important.

3 Type of actor

In this section the type of actor that is relevant for this scenario will be proposed and the underlying three factors that cause a variance in the metrics will be discussed.
The type of actors whose security performance is visible are the customers in the countries in which the Autonomous Systems are located.

3.1 Underlying factors

The underlying factors that can cause a variance in the metrics are the following (Van Eeten et al. 2010):

- The country where the AS is located
- The size of the AS company or network
- The number of customers
- The type of websites that the AS hosts
- The costs spent by the AS on security (investment of the company)
- The legal implications and regulations that hold for the AS
- The competition of the AS
- The costs of the customer support that the AS provides
- The behaviour of the customers (security awareness, online activities)
- The education and income level of the customers
- The reputation of the AS

3.2 Data collection

The technology index[1] will be used for the purpose of gathering additional data to get better insights into this problem. The technology index is a country-level statistic based on factors like company spending on R&D, and personal computer and internet penetration rate, among others. We expect countries with high technology index, meaning a larger adoption of technology and more of the population being exposed to the internet, to be a greater target for website defacements.

As a measure for population education, the education index[2] is used. The education index uses the average amount of years of schooling and expected years of schooling. With a more educated population we expect a higher level of security and thereby a lower defacement count.

3.3 Statistical Analysis

In this subsection a statistical analysis will be performed in order to explore the impact of these factors on the metric.
For the statistical analysis we have chosen to use the Pearson correlation coefficient [3]. This correlation coefficient measures the statistical relationship between two continuous variables. In order to be able to use the Pearson correlation on the dataset, we first plotted the data to see if it was normally distributed. The Pearson correlation is calculated with the following formula:

$$\rho = \frac{cov(X, Y)}{\sigma_x \sigma_y} \tag{1}$$

The Normalized Defacement count per country indicates the security level of the network of all AS providers per country. This value is calculated as the average count of normalized defacements per month for each country.

3.3.1 Normalized Defacement count per country correlated with technology index

In order to calculate the correlation between the Normalized Defacement count per month and the Technology index, the data needs to have a normal distribu-

[1] https://www.nationmaster.com/country-info/stats/Economy/Technology-index
[2] http://hdr.undp.org/en/content/education-index
[3] https://www.statisticssolutions.com/pearsons-correlation-coefficient/

tion, this can be seen in Figure 1.

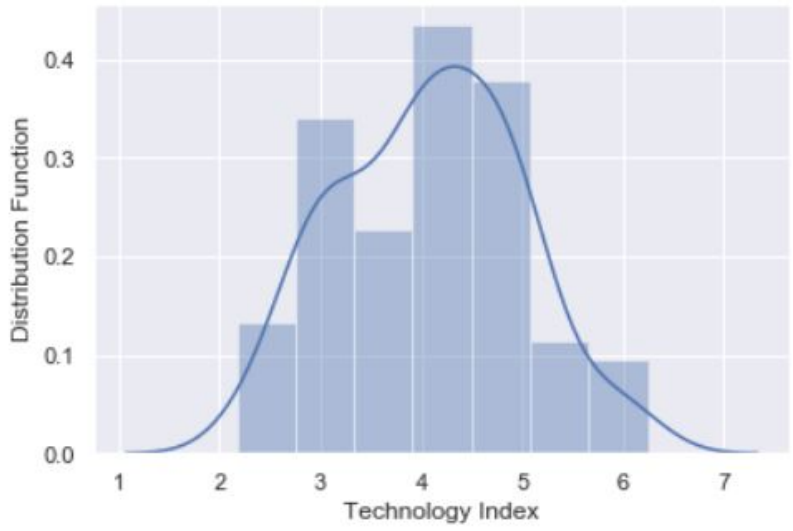

Figure 1: Distribution of Technology Index

The correlation between the Normalized Defacement count and the Technology index is

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2(y_i - \overline{y})^2}} = 0.040632274632839804.$$

The corresponding p-value is 0.7021595330558136.

Because the correlation coefficient value is approximately 0.04, this means that there is a very low correlation between the two variables. Also the p-value is greater than 0.05 which confirms that the significance is very low.

3.3.2 Normalized Defacement count per country correlated with education index

In order to calculate the correlation between the Normalized Defacement count per month and the Education index, the data needs to have a normal distribution, this can be seen in Figure 2. The correlation between the Normalized Defacement count and the Education index is

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2(y_i - \overline{y})^2}} = -0.10370821896006371.$$

The corresponding p value is 0.1990820598193796. The value of the correlation coefficient is approximately -0.103 which indicates that there is a low correlation

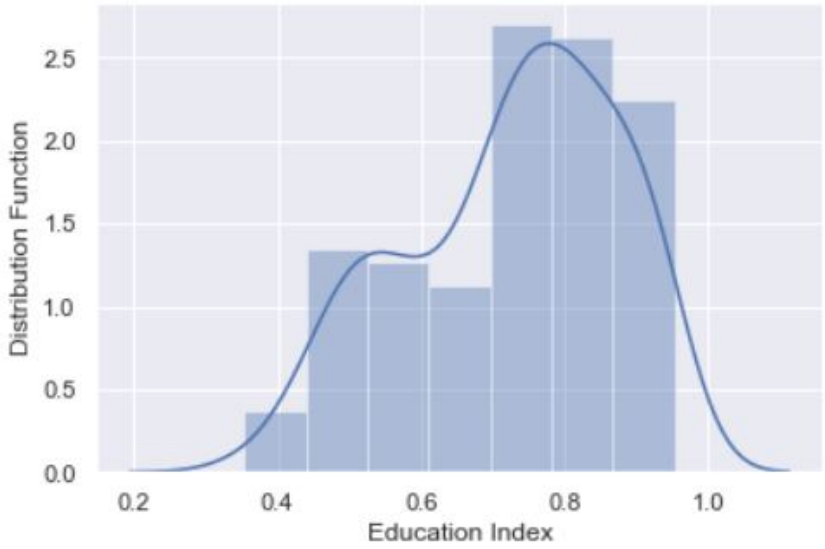

Figure 2: Distribution of Education Index

between the education index and the number of defacements. The p-value which is 0.1 also indicates that this correlation is not significant.

4 Conclusion

We have investigated some factors that we believed influenced the Normalized Defacement count. The factors we have analysed are the technology index and the education index per country. To measure the correlation between those factors and the Normalized Defacement count a Pearson correlation coefficient is used. However, the Pearson correlation coefficient showed that neither the education-index, nor the technology-index, are significantly correlated. The obtained results indicate that the level of education per country does not play a significant role in the security awareness amongst customers. The technology index which represents the technological readiness of a country also does not have a significant influence on the number of security incidents in that country.

References

Renda, A et al. (Dec. 2013). *ASSESSING THE COSTS AND BENEFITS OF REGULATION*. URL: https://ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/131210_cba_study_sg_final.pdf.

Van Eeten, Michel et al. (2010). “The role of internet service providers in botnet mitigation an empirical analysis based on spam data”. In: TPRC.