Economics of cybersecurity

Databreaches, Assignment block 4 Draft

Group 5: Hasan Abdullah - 4614097, Seu Man To - 4064976, Elsa Turcios Rodriguez - 4597818, Tim van Rossum - 4246306

In the previous assignment we have analyzed the variance in security performance in relation to a metric and how different risk strategies can shape this variability. This assignment aims at understanding the factors influencing this variance, i.e., instead of analyzing what the differences among different actors are we will investigate the underlying reasons behind the existence of these.
Actors involved in the security issue follow different strategies to mitigate its impact. For this assignment:

1 Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment). For each one:

The three actors chosen are: the healthcare industry (the problem owner), the government, and the security providers.

1.1 Identify one concrete countermeasure that they could take to mitigate the security issue,

Actor	**Countermeasure**
Healthcare Industry	Data Encryption
Government	Enforcement of the current data breach disclosure law
Security Providers	Apply Standards to product development

Table 1: Actors with their countermeasure

Healthcare industry: Data Encryption. Although encryption cannot prevent an attacker to steal physical device or data, encryption can protect the information by making it unreadable to the attacker. Also, as it will be explained in question 1.3 the healthcare industry has incentives to apply this countermeasure.

Government: Enforce the current data-breach disclosure law. Organizations and firms need incentives to protect their customers' data, so somehow they will need the government to push and keep them in track.

Security providers: Apply Standards such as IEEE, ISO, HIPAA to the products they develop for the healthcare industry to ensure right level of security. The use of standards can reduce the information asymmetry regarding the quality of the products or services that security providers offer to the healthcare industry, so the healthcare industry can make better decisions about which products or services to use to protect data.

1.2 Analyze the distribution of costs and benefits among the different actors that the deployment of the countermeasure would entail.

Actors have to perform a cost benefit analysis in order to decide to follow a countermeasure or not. The cost is the effort to follow the countermeasure such as monetary, time, and the benefit is the avoidance of the harm that the countermeasure can bring (Herley, 2009). In the next table, the actors will be depicted with the cost they have to incur to implement the countermeasures selected, and the benefits of applying them.

Actor	Cost	Benefit
Healthcare Industry **(Encrypting data)**	Deployment cost of encryption including software, hardware, and installation	Secure data
	One-off productivity loss during installation	Attackers will have to obtain the decryption key as well to make the data readable
	Training of personnel	Avoid liability cost such as fines and demands due to data breaches
	Secure decryption key storage	
Government	Monitoring the compliance of the law	Data available to reduce asymmetric information among companies in the

(Enforce the current data-breach disclosure law)		healthcare industry (Moore, 2010).
	Extra administrative costs to enforce the law	Users have the opportunity to take actions once a data breach in the healthcare industry happens (Moore, 2010).
		Healthcare industry will take security measurements to prevent data breach more seriously
Security Providers (Apply Standards)	Obtention of Certificate	Standard products meeting security requirements
	Training of the personnel	They can differentiate their product vs competitors which are not certified

Table 2: Actors with their costs and benefits.

1.3 Analyze whether the actors have an incentive to take the countermeasures

The healthcare industry has an incentive to implement encryption of data. In February 2009, HITECH Act (Health Information and Clinical Health) has been passed in The United States. The law mandates the notification of unauthorized disclosure of patient-protected health information (Trend Micro, 2012). But the law exempt the need to report the loss, if the data is encrypted. This creates incentive for encryption in healthcare industry. On the other hand, because the goal of the medical staff is to save lives and provide care to patients, implementing the countermeasure might slow down the tasks of the medical staff. Therefore, this can be an incentive to avoid the implementation of the countermeasure. Nevertheless, in financial terms and the liability cost that the healthcare industry can avoid implementing the proposed countermeasure the benefit lead to a high incentive to implement it.

The government has the task of ensuring cyber security in cyberspace. "Problems plaguing cybersecurity are economic in nature, and modest interventions that align stakeholders incentives and correct market failures can significantly improve a nation's cybersecurity posture" (Moore, 2010, Pag.2) In this case, the role of the government enforcing the current data breach law provides incentives to the healthcare industry to improve its cybersecurity and improve the safety of the data and correct information asymmetry among the different companies in the healthcare industry. Therefore, the incentive of the government is to improve the security posture of the healthcare industry to invest in security upfront (Asghari, 2016).

Also, security providers have incentive to implement the proposed countermeasure, as they want to stay ahead of the competition with other security providers to get more customers. Inability to comply with the required standards to deliver products or services to the healthcare industry might cause them to lose clients and not be able to compete with the competitors, which lead to reduced revenues. Therefore, the market competition is an incentive to apply the countermeasure.

1.4 Briefly reflect on the role of externalities around this security issue.

Implementing the countermeasures would create a positive externality for the patients, as it offers better security for their personal data. In addition, enforcing the data-breach law creates both a positive or negative externality for law enforcers: law enforcers get more responsibilities, a negative externality, but they logically get paid more as well due to their extra responsibilities (this would logically motivate them to ask for a raise), a positive externality. Security providers adopting standards for their security creates a positive externality for organizations in charge of creating standards. Their standards will become popular and accepted through the industry and they will get benefits from it.

2 Identify the type of actor whose security performance is visible in the metric(s) you selected (e.g. ISPs, software vendors, countries). Note that this is not necessarily the problem owner, rather is the unit of analysis in your metric.

The type of actor selected is the types of industries, and the unit of observation will be the number of data breaches per industry. It is important to notice that the number of data breaches per industry is not normalized. Therefore, the conclusions drawn after the statistical analysis might not be accurate.

2.1 Identify different factors explaining (causing) the variance in the metric.

The dataset shows the number of data breaches based on the type of industry. A literature review has been conducted to explain the variance of the number of data breaches per industry.

One of the factors that can affect the number of data breaches experienced per industry is the black market data cost. Due to the fact that the healthcare industry possesses more documented data that can help to identity theft and attackers can make profit through direct sale, and this data can also be used for extortion (Czeschik, 2017). Therefore, the healthcare industry is an attractive target.

A second factor identified is the security investment that each industry spends in cybersecurity. As the need for IT security professionals are becoming more demanding, the salaries are increasing. Therefore, budget issues to hire expert professionals could be a cause to the number of data breaches (Wired, 2015). In addition, the lack of qualified personnel in cybersecurity area also can contribute to the number of data breaches (Cisco, 2017). Nevertheless, it is difficult to find data about which industries experience more problems with finding qualified personnel in this area.

Another factor that can possibly affect the variance is the size of the industry and the nature of the core of their businesses. There are industries composed of more companies, or serve high amount of clients, or offer different services.

Therefore, the amount of people involved or the size of the operation of each industry can play a role in the variance of the number of data breaches.

2.2 Collect data for one or several of these factors

Data of the three variables explaining the variance of the metric: black market price, cybersecurity investment per industry, and size of the company was tried to be obtained through literature review. It was difficult to find data about those factors. Nevertheless, below are the data that have been successfully gathered to try to understand these factors:

Security investment per industry to IT

The ideal situation will be to obtain public data about the investment in cybersecurity of companies that were breached as well as the size of the company, so that it would be possible to build more accurate metrics about the industry. Nevertheless, there is no information available about them. The data that was found is the IT budget allocated per industry, but this data was only 72% US data. It will be assumed that this data is 100% from United States. In addition, in the majority of the cases there is a range of investment not a specific amount, so the median of the investment in IT is calculated.

Industry	2014	2015	2016
Financial services	$1M	$500K-$1M=$750K	$500K-$1M=$750K
Technology/IT services	$100K	$100K-$500K=$300K	$100K-$500K=$300K
Government	$500K-$1M=$750K	$500K-$1M=$750K	$1M-$10M=$5.5M
Education	$1M-$10M=$5.5M	$1M-$10M=$5.5M	$1M-$10M=$5.5M
Health care	$1M-$10M=$5.5M	$1M-$10M=$5.5M	$1M-$10M=$5.5M

Table 3: Median budget allocated to IT (SANS Institute InfoSec Reading Room, 2016)

Since finding the budget allocated specifically to cybersecurity per industry was not possible, the IT budget was used in combination with another source (Table 4) which give details about the percentage of IT budget allocated to security per industry. So using the median of the percentage and the IT budget made it possible to calculate the cybersecurity spending per industry (Table 5).

Industry	2014	2015	2016
Financial services	7%-9%=8%	7%-9%=8%	10%-12%=11%
Technology/IT services	1%-3%=2%	4%-6%=5%	4%-6%=5%
Government	4%-6%=5%	4%-6%=5%	7%-9%=8%
Education	1%-3%=2%	3%-4%=3.5%	1%-3%=2%
Health care	4%-6%=10%	4%-6%=5%	4%-6%=5%

Table 4: Percentage of IT budget allocated to security (SANS Institute InfoSec Reading Room, 2016)

Cybersecurity Investment per industry

Industry	2014	2015	2016
Financial services	$80,000	$600,000	$82,500
Technology/IT services	$2,000	$15,000	$15,000
Government	$37,500	$37,500	$440,000
Education	$110,000	$192,500	$110,000
Health care	$550,000	$275,000	$275,000

Table 5: Calculated security investment per industry

Size of industry

Determining the size of the industries is not easy to accomplish. Therefore, an idea to measure the size is to look for the value added of each industry to the GDP of the United States. "Value added is the contribution of each industry's labor and capital to its gross output and to the overall gross domestic product (GDP) of the United States" (Bureau of Economic Analysis, BEA, 2017). The higher the value added, the bigger the industry will be considered.

Industry	2014	2015	2016
Financial services	$1.251.154M	$1.293.093M	$1.355.546M
Technology/IT services	$338.726M	$373.239M	$396.342M
Government	$2.277.257M	$2.337.979M	$2.391.563M
Education	$195.145M	$202.251M	$207.321M
Health care	$1.223.155M	$1.298.901M	$1.368.697M

Table 6: Value added per industry (Bureau of Economic Analysis, BEA, 2017)

2.3 Perform a statistical analysis to explore the impact of these factors on the metric.

In the first assignment the metric revealed that the healthcare industry had a higher amount of data breaches compared to the other industries. Therefore, the intention of a statistical test will be to answer to the following research question:

To what extent does cybersecurity investment and size of the industry correlate to data breaches?

To answer this question the following steps should be followed:

1) Literature review to identify variables that can cause the variance.
2) Data collection of the independent variables.
3) Develop a conceptual model and hypothesis to test.
4) Data Analysis.
5) Interpretation of the data to answer the research question.

Figure 1 and 2 are graphs related to the metrics of the first assignment where it is possible to observe the difference in the amount of data breaches per industry.

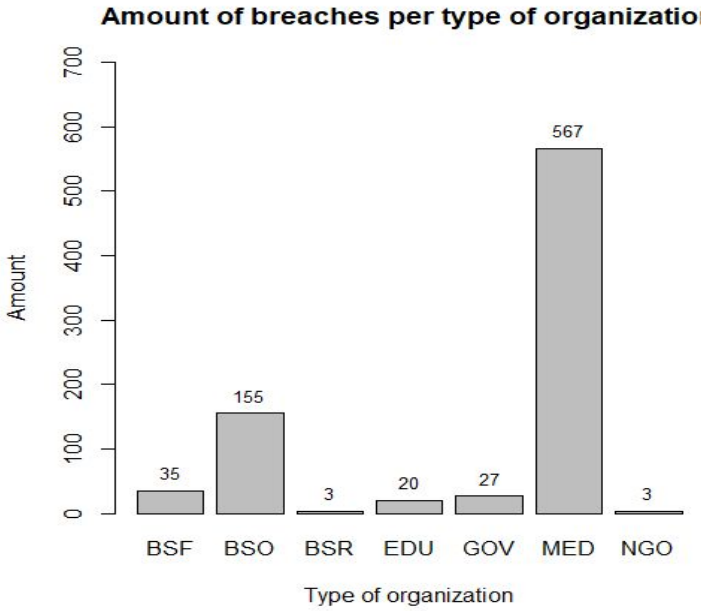


Figure 1: Amount of data breaches per industry

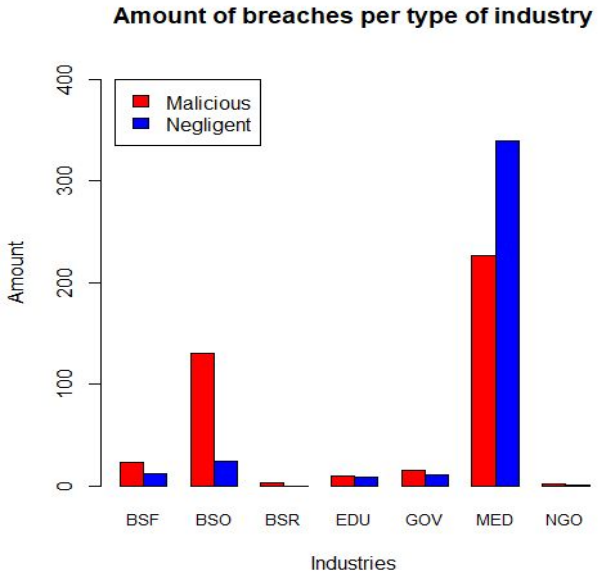


Figure 2: Amount of data breaches classified by Negligent and Malicious per industry.

Steps 1 and 2 were conducted in section 2.1 and 2.2 respectively, and now step 3 to answer the research question follows:

2.3.1 Conceptual Model

Through literature review, the independent variables defined are: Budget Spent in Cybersecurity per industry and Size of the industry. Unfortunately, it was not possible to obtain the cost of data records on the black market per industry because the prices found in the literature review only set the price of certain records that can come from any industry. Therefore, only two variables will be used to create a conceptual model of how it would be possible to see if a correlation exists.

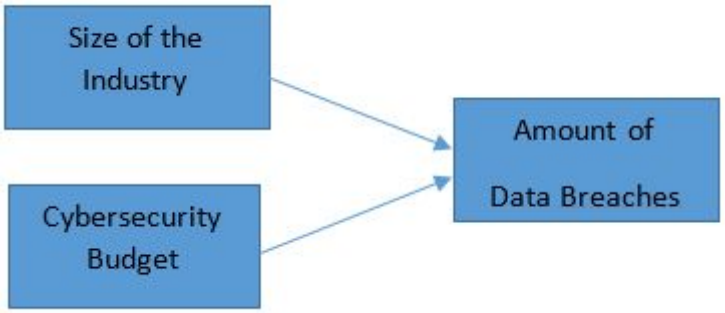


Figure 3: Conceptual Model of the Dependent and Independent Variables

From this conceptual model the following hypotheses are developed. Where HA is Alternative Hypothesis and H0 is Null Hypotheses.

HA1: The size of the industry is correlated with the amount of data breaches.
H01: There is no correlation between the size of the industry and the amount of data breaches.

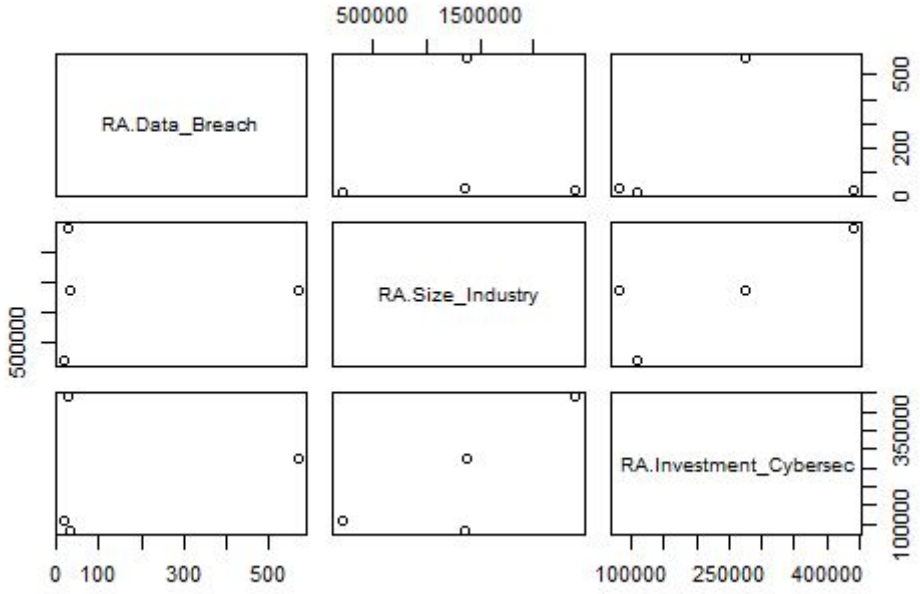
HA2: The budget spent in cybersecurity is correlated with the amount of data breaches
H02: There is no correlation between the budget spent in cybersecurity and the amount of data breaches.

2.3.2 Data Analysis

To answer the research question, a pearson correlation analysis has been performed. The data related to the independent variables collected and the data set of the Privacy Rights Clearinghouse dataset were combined.

	Industry	Data_Breach	Size_Industry	Investment_Cybersec
1	Bsf	35	1355546	82500
2	Gov	27	2391563	440000
3	Edu	20	207321	110000
4	Med	567	1368697	275000

Correlation Analysis:



	RA.Data_Breach	RA.Size_Industry	RA.Investment_Cybersec
RA.Data_Breach	1.0000000	0.0394896	0.1913297
RA.Size_Industry	0.0394896	1.0000000	0.8022386
RA.Investment_Cybersec	0.1913297	0.8022386	1.0000000

2.3.3 Interpretation of the data and Limitations

There is a weak positive correlation of 0.19 between Investment in cybersecurity and the amount of data breaches per industry and also a weak positive correlation of 0.039 can be observed between the size of the industry and the amount of data breaches. Nevertheless, it is clear that correlation is not causation, and the initial thoughts when collecting this information was to perform regression analysis to understand how much each independent variable contribute to the number of data breaches per industry. But due to the sample size and that these variables did not meet a linear relation with the number of breaches it was not possible to perform this analysis. If there was data available of the budget spent in cybersecurity per company breached, then each company could be an observation of the industry and if a better metrics of the size of the companies breached were available then this could be aggregated to define the size of the industry. Then it might be possible to conduct a better study.

In addition, these results are only based on 4 observations with a small sample. The limitations encountered to collect data to perform the statistical analysis

hinders the conclusions of it. In this case, the analysis is relying on data that was assumed to be 100% from United States. Also, since the resources of data are limited, the data only comes from one single source, therefore triangulation of the information is not possible. In addition, the amount of data breaches is not normalized. Besides, only four industries could be compared because no data of other industries have been found. It is not impossible to conclude anything from the correlation results only that the two independent variables proposed: Cybersecurity Investment and Size of the industry are not correlated with the number of data breaches experienced by industries.

One of the main issues trying to perform a statistical analysis for this dataset was the lack of data available to add to the Privacy Clearinghouse dataset and come up with a meaningful analysis. It is possible that data is not available due to the sensitivity of this information as well as the lack of incentives to make data public.

References

Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144). ACM.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3), 103-117.

Trend Micro. (2012). Addressing the Data Protection Requirements of the HITECH Act

SANS Institute InfoSec Reading Room. (2016). IT Security Spending Trends

Czeschik C. (2018) Black Market Value of Patient Data. In: Linnhoff-Popien C., Schneider R., Zaddach M. (eds) Digital Marketplaces Unleashed. Springer, Berlin, Heidelberg

Wired. (2015). The Root of the Problem: How to Prevent Security Breaches. Retrieved from https://www.wired.com/insights/2015/02/the-root-of-the-security-problem/

Asghari, H. (2016). Cybersecurity via Intermediaries: Analyzing Security Measurements to Understand Intermediary Incentives and Inform Public Policy. Doctoral thesis. doi:10.4233/uuid:3694edf5-d6e0-4484-b847-750da2b9d1b9

Bureau of Economic Analysis, BEA. (2017). Gross Domestic Product (GDP) by Industry Data
Retrieved from https://www.bea.gov/industry/gdpbyind_data.htm

Cisco. (2017). Retrieved on October 15th, 2017 from https://continuum.cisco.com/2017/06/09/cybersecurity-will-have-a-workforce-gap-of-1-8-million-by-2022/