Economics of cybersecurity

Databreaches, Assignment block 3

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

1 The Problem Owner

The problem owners of malicious and unintended data breaches are the different industries, but for this assignment the scope will be narrowed down to the healthcare industry as the problem owner. The healthcare industry is chosen, because in the previous assignment this industry had the most counted data breaches. It is worthy to clarify that the normalization of the data set used for the assignment is not easy to attain since the data is compared through different industries. Therefore, it is hard to come up with a method to normalize the comparison among industries because they have different characteristics, core business, and size. Therefore, the use of counts is made. Meanwhile the authors of this report are thinking in possibilities to normalize it for the next assignment.

2 Relevant differences in security performance

The relevant differences that the metrics revealed is that the healthcare industry has the higher count of data breach incidents, and this industry is more affected by negligent data breaches compared to other industries that are only affected by malicious data breaches. Nevertheless, it is difficult to conclude that the security performance of the healthcare industry is poorer than the other industries because the data breaches count among industries is not normalized yet.

3 Risk strategies to reduce the security issue

The healthcare sector stores data of their customers (medical records of patients, private information of patients, et cetera). These data are a valuable asset and should not fall into the wrong hands. Such event will cost the healthcare industry a huge amount of direct (such as ransom of data) and indirect cost (reputation). The main strategy that security consumers like the healthcare industry can follow to

reduce the security issue, which is malicious and unintended data breaches, are constrained by budget allocation. Nevertheless, there are some strategies that they can adopt to reduce the security issue at hand:

- Follow and oblige security standards and compliance as a base security control to avoid liability.
- Security training and awareness for medical staff to avoid negligent issues.
- Based on Symantec report (Symantec, 2016), compared to other industries, the healthcare industry has the lowest percentage of IT security budget over the whole IT budget. This was caused by the lack of understanding of their executives of the threats facing their organization (Cisco, 2015). That is why there is a need for re-prioritizing IT security budget and create awareness of understanding cyber security in terms of risk on the executive level.
- Cisco (2015), on its report mentioned that compared to other industries, healthcare does not have the full architecture of strong security defenses. Healthcare organizations only prioritize more on the edge of the network that is only related to outsider attack. Healthcare organizations need to implement an IT security architecture which also monitors the inside of networks, so if someone has access to critical systems, they can limit the impact. This can be done by several strategies. First, through a proper network segmentation to block unwanted access from unwanted persons. Second, by deploying encryption for important data. By doing so, even though someone gains access to valuable information, it cannot easily be opened.

4 Actors that can influence the security issue

The main actor that can influence the security issue, malicious and unintended data breaches, is the healthcare industry. Especially the personnel working in the healthcare sector can play an important role. The personnel can be divided in two groups. First, Medical Staff which is composed by doctors, nurses, and medical personnel that provides care to patients. Second, Technical Staff which will be assumed to be composed by IT and Cybersecurity staff in charge of the security of data records. The Medical Staff can be trained and be aware of how to prevent unintended data breaches, while IT and Cybersecurity staff can implement technical

solutions to influence the security issue. In both cases, it will be considered that they can impact the security issue in a positive way to avoid it. The personnel can help with implementing best practices and complying with security standards.

Other actors that can influence the security issue in different manners are depicted in Table 1.

Actor	**How can influence the security issue**	**Impact**
Attackers	The behavior of attackers can influence the amount of breaches the healthcare industry can suffer.	Positive/Negative
Security providers	Develop solution to improve security of the Healthcare industry.	Positive
Security Industry	Selling security that prevent these type of breaches (Unintended and Malicious).	Positive
Government	Government can enforce compliance to the healthcare sector to reduce the security issue.	Positive
Crypto markets	Create a place to trade the data; creating incentive for the demand of the data.	Negative

Table 1: Actors that can influence the security issue

5 Risk strategies that the actors can adopt to tackle the problem

The main strategy of the healthcare industry can be adoption of best practices and compliance of industry standards as it was expressed in the previous section. In addition, the different actors involved in the security issue at hand can adopt and have different strategies to tackle the problem.

First of all, security providers can develop better security measures for the healthcare industry. The main strategy security providers are using to serve the healthcare industry is a growth strategy with emphasis on adding convenient and visible features for their users. Since the medical staff's core capabilities are

oriented to serve patients and not to learn technicalities, the security providers need to ensure an easy way of using their products to increase the likelihood of adoption in this sector. Nevertheless, this growth strategy needs to be combined with the right amount of efforts in cybersecurity to ensure that the growth strategy does not undermine security. Therefore, the use of security providers certificate can be an option to incentive growth, but at the same time tackle the security issue at hand.

Second, government can ensure policies that enforce the protection of data, so that the healthcare industry increases security of the data of their customers. The main strategy of the government is policy creation to ensure sharing data about data breaches in the healthcare industry.

Third, it is not possible to determine strategies from the perspective of attackers and the crypto market to tackle the security issue since they are part of the problem, and they are getting benefits from it. Therefore, they do not have an interest in solving the problem.

6 Strategy changes of the actors over time

The strategy of the government has changed over time because of the rapid development of IT and Cyberspace. In the past the government did not have to worry about policies to ensure data protection. Present day, there are policies to protect data. In this particular case the evolution of the strategy of the government has contributed to reduce the risk.

In the case of the security providers, the strategy regarding adding convenience and visibility to the development has contributed to increasing risks. Through time security providers have been competing to serve the healthcare sector. Therefore the mentality ‘ship now and fix later’ to increase their growth or to deliver user oriented developments can lead to overlooking the security of their final products. Therefore, certification of the security providers is necessary nowadays to decrease this risk.

In the case of the attacker and cryptomarkets no strategies were described, but what can be observed is that in the past, the reach of an attacker was probably less when internet connection did not exist. In addition, in the past cryptomarkets did not exist. Therefore, these two actors have created an increase in the risk for the healthcare industry.

7 Return on Security Investment (ROSI) for Encryption

Cryptosystems (encryption) has been chosen as the strategy that the main actor, the healthcare industry, can follow to reduce malicious and unintended data breaches. First, an estimation of the costs is given and then an estimation of the benefits is given.

7.1 Estimate the costs involved in following that strategy

Costs for implementing a cryptosystem for the data: this is quite hard to estimate, due to there being a lot of ways to implement such a cryptosystem. Thus a lot of different costs per system to take into account.

The cost of full disk encryption on laptop and desktop computers in the United States including hardware and software full encryption is $483.4 per disk (Ponemon Institute, 2013). It is not clear if some of the cost are annually expressed, but it will be assumed that all the costs are estimated annually. Further it is necessary to consider that "the cost of the solution is not just what is written in the price" (Sonnenreich, Albanese, & Stout, 2006, p.52). Therefore, this cost has already included activities that can impact the productivity loss due to idle time for password resets, idle time due to initial encryption, and excess time operating computer. The problem here is that a database of healthcare institutions could potentially have many disks and it is not known how many disks make up a single database for a healthcare institution. It will be assumed that 50 disks per database server are used, and that every disk can contain about 2 TB of data, giving us a data capacity of 100 TB per database server (this should be more than enough for even the biggest healthcare institutions).

US Sample	Hardware FDE	Software FDE
Licensing cost	$2,5	$8,1
Annual Maintenance	$1,0	$15,0
OPAL Fee	$7,9	-
Tech cost to pre-provision computer	$1,3	$1,3
Tech cost to stage computer	$12	$12
Tech cost to reset password	$4,5	$4,5
Tech cost to re-encrypting after re-imaging	-	$1,8
Tech cost of special administration	$0,3	$0,3
Impact on Productivity		
Value of idle time due to password reset	$22,2	$22,2
Value of excess time operating computers	$23,1	$323,4
Value of idle time due to initial encryption	-	$30
	$74,8	$408,6

Table 2: Cost of Full Encryption Including Loss on Productivity

Adapted from Ponemon Institute, 2017, p.5

Solution cost including productivity loss assuming that 50 disks are used in a server in a healthcare institution per year:

	Cost per Disk	Amount of disks assumed	Total Cost annually
Full disk encryption	$483,4	50 Disks	$24.170

7.2 Estimate the benefits of following that strategy

In order to make sensible estimations of the benefits of following a certain security strategy, some values and functions have to be defined and estimated first:

Annualized Expected losses (ALE) = Impact (Unit) * Probability (annual).
ALE_o = without security measures in place (original scenario)
ALE_s = with security measures in place (secured scenario)

ROSI = (benefit - cost) / cost = (ALE_o - ALE_s - c) / c.

ALE_o is estimated as follows: from the original dataset, it can be deduced that on average, around 40.000 records are breached per data breach. However, this is not really sufficient in itself as it does not take into account different sizes of healthcare facilities. As such, the amount of records breached were grouped by order of magnitude to come up with a reasonable loss distribution. The loss distribution is given in figure 1.

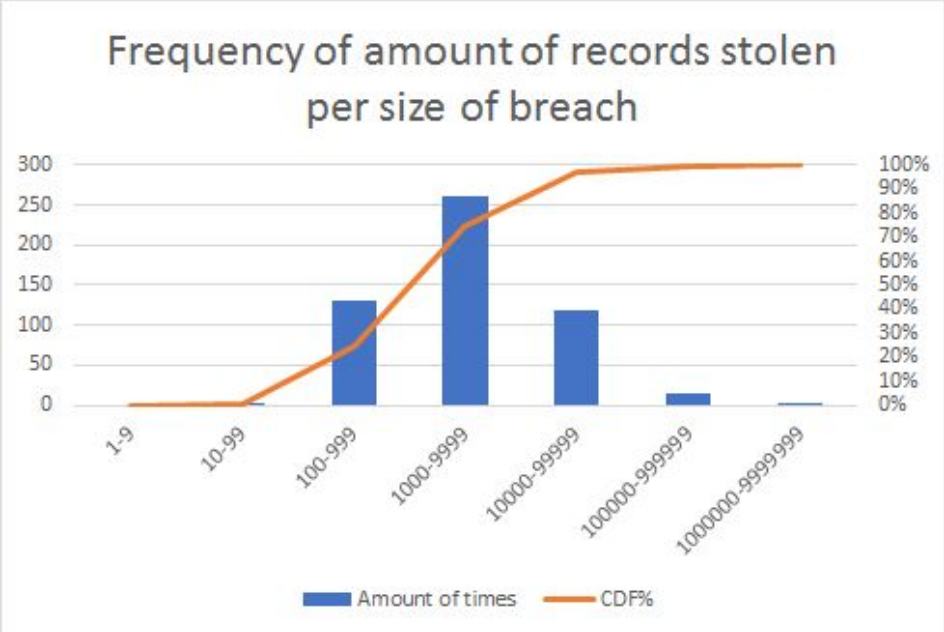

Figure 1: the frequency of breaches per size of the breach.

As can be seen in the data, breaches ranging between 1000 and 9999 records are the most common, differing from the average of 40.000 by about an order of magnitude. For ROSI calculation, the average of the most common range of records breached will be used, which is 5000.

As for the cost for the company in the case of a data breach: a study (Ponemon Institute, 2017) showed that the average cost of a breached record for a company is around $154, but this average is higher for medical records, with medical records costing a medical facility up to over $300. Using this, a reasonable average would be $200, taking into account that not all records are sensitive.

As for the probability that a certain company will be breached: according to AHA (2017), there are 5564 registered hospitals in the US. There are 529 different medical facilities in our dataset. Using this, the probability of a medical facility being attacked is calculated to be 529/5564 = 0,095 (approximately). Because not all medical facilities are hospitals, the amount of medical facilities in the US is even greater than 5564, thus the probability of being attacked decreases and a conservative estimate for that probability would be 0,08, resulting in ALE_o = $200 * 5000 * 0,08 = $80.000.

Now for estimating ALE_s: Focussing only on encryption strategy, the probability will not decrease as it is not meant to prevent attacks. Attacks will continue as normal. The main focus is on the impact: attackers now need to steal the decryption key too in order to use the data for their own gain. A reasonable assumption of the amount of records that can still be read after an attack is around 10%.

This reduces the impact to $80.000 * 0,1 = $8.000, resulting in ALE_s = $8.000.

The ROSI can now be calculated as follows:

$$ROSI = \frac{\$80.000 - \$8.000 - \$24.170}{\$24.170} = \frac{\$47.830}{\$24.170} = 1,98 = 198\%$$

8 Conclusion

This ROSI is, of course, only an average, using a median of the amount of records breached. There is absolutely no way of telling whether or not a medical facility will be attacked in the next year, whether or not attackers can read any data at all after they have broken into the system and obtained some records, or even whether or not encryption standards will be better next year. However, using average and median values, the investment does seem to be beneficial. Nevertheless, this strategy needs to be accompanied by other strategies such as cultural values and awareness of the personnel in the healthcare industry, because full encryption can lead to moral hazard problems such as employees behaving more reckless because of the sense of security (Asghari, van Eten, Bauer, 2016).

Looking only at ROSI, we can already see that, for an average case using a rough median of the amount of records breached, the investment has a high ROSI, indicating that the investment is beneficial. However, as mentioned, the investment might be worthless down the line due to encryption standards possibly being outdated within the year. As such, we decided to compare the benefits of this strategy with a different strategy: network segregation.

Network segregation is the act of segmenting parts of the internal network of the system, so that one cannot access at least one part of the system from any other part. This could be used to store data in a system part completely cut off from the rest of the system. One benefit using this strategy would be the fact that the upfront cost would most likely be limited, as using this strategy would involve parts of the internal network being disconnected from each other, requiring no added hardware or the like. One very major downside is the potential impact it has on the productivity of the workforce in the facility. As data cannot be sent to the main database from other computers in the facility, it has to be written down somewhere first in order to be stored later (which can also cause accidental data leaks in itself). This causes employees to lose time they could have spent being productive. In this case, the loss of productivity happens not once, but every single time a

new record has to be entered into the database. This can add up quickly, depending on the size of the workforce. It might also be pointless to even segregate the network in the first place, as the facility might never be attacked.

In the end, it all really depends on the circumstances at hand and no strategy is going to be the absolute best in every single case. The benefits of data encryption do seem to outweigh the disadvantages, especially compared to the potential massive productivity loss incurred by segregating the network. As such, the estimated benefits of encryption compared to other strategies would be both high ROSI and a relatively low, only initial, impact on productivity.

References

Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity. *Chapters*, 262-287.

Cisco. (2015). Cybersecurity in Healthcare: Why It's Not Enough, Why It Can't Wait.

NETWORKComputing. (2012). Calculating the Cost of Full Disk Encryption. Retrieved from http://www.networkcomputing.com/careers/calculating-cost-full-disk-encryption/1443138451

Ponemon Institute. (2017). 2017 Cost of Data Breach Study AHA. (2017). Fast Facts 2017. Retrieved from http://www.aha.org/research/rc/stat-studies/fast-facts.shtml

Ponemon Institute. (2013). The TCO of Software vs. Hardware-based Full Disk Encryption Summary.

Sonnenreich W., Albanese J., & Stout B. (2006). Return on security investment (ROSI) - A practical quantitative model. Journal of Research and Practice in Information Technology, Vol.36, No.1.

Symantec. (2016). Healthcare Security: Improving Network Defenses While serving Patients