Economics of cybersecurity

Databreaches, assignment block 2 draft

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

1. Who is the problem owner of the security issue as measured in your first assignment?

The problem owners are the different industries, but for this assignment the healthcare industry will be defined as the problem owner. The healthcare industry is chosen, because in the previous assignment this industry had the most counted data breaches.

2. What relevant differences in security performance does your metric reveal?

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

3. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

Healthcare sector stores data of their customer (patient's' medical record, patient's private information, etc). These data are a very 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 healthcare industry follows are constrained by budget allocation.

Some of the strategy that they can adopt:

- Follow and oblige security standards and compliance as a base security controls to avoid liability.
- Security training and awareness for medical staff to avoid negligent issue

- Based on Symantec report (Symantec, 2016), comparing to other industry, healthcare 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 of re-prioritizing of IT Security budget and create awareness of understanding cyber security in term 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 only related to outsider attack. Healthcare organizations also 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. Such can be done by several strategy. First, through a proper network segmentation, to block unwanted access from unwanted person. Second, by deploying encryption for important data. By doing so, even though someone gain access to valuable informations, it cannot easily be opened.

4. **What other actors can influence the security issue as measured in your first assignment?**

The main actor that can influence the security issue are the personnels working in the healthcare industry. The personnels can be divided in two. 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. Other actors that can influence the security issue are:

- Attackers: the behavior of attackers can influence the amount of breaches the healthcare industry can suffer.
- Security providers: develop solution to improve security.
- Security Industry: selling security.
- Government: government can enforce compliance to the healthcare sector.

- Crypto markets: create a place to trade the data creating incentive for the demand of the data.

5. **Identify the risk strategies that the actors can adopt to tackle the problem**
    1. **are there actors with different strategies? Why?**

Attackers do not tackle the problem, as they are part of the problem.

Cryptomarkets do not tackle the problem either, as they are a trading place and they do not care about the problem.

Security providers will develop better security measures for the healthcare facility. The main strategy of security providers are using to serve healthcare industry is a growth strategy with emphasis in adding convenient and visible features for their users. Since the medical staff core capabilities are oriented to serve patients and not to learn technicalities, the security providers need to ensure easy way of using their products to increase the likelihood of adoption in this sector.

Government can ensure policies that enforce the protection to data, so that healthcare sector increases security of the data of their customers. The main strategy of the government is policy creation to ensure a better society.

2. **have the strategies changed significantly over time in a way that reduces or increases risks?**

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 and know 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 case of Security provider the strategy regarding adding convenience and visibility to the development has contributed to increasing risks.Through the time security providers have to compete to serve the healthcare sector, so the option ship now and fix later to increase their growth or to deliver user oriented developments can lead to overlook the security of their final products.

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

6. **Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,**

Cryptosystem (encryption) has been chosen as the strategy and the calculation will be as follows:

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 and thus a lot of different costs per system to take into account.

The cost of full disk encryption on laptop and desktop computers is $235 per year (NETWORKComputing, 2012). The problem here is that a database could potentially have many disks and it is not known how many disks make up a single database. 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 hospitals). Encrypting every disk costs $11.750, and there is probably a very small impact on productivity. Therefore, it will be assumed that the impact cost in productivity will be $3.250. Due to this, the estimated total cost of encrypting all data disks to be around $15.000.

However, this cost does not take into account laptops from personnel that have disks to be encrypted, maintenance costs, desktops used in the facility that have disks to be encrypted, all the productivity loss because of personnel having to hand in hardware, etcetera. Factoring these in, the cost can quite easily surpass $30.000 making an assumption. Because it is possible that other factors are being omitted the cost that will be used to calculate ROSI will be $40.000.

2. **Estimate the benefits of following that strategy (assume a particular loss distribution)**

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)

$EBIS_s = ALE_o - ALE_s$.
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 100.000 records are breached per data breach. 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 $100, taking into account that not all records are sensitive. Because no data is encrypted, all breached records can be easily seen, and the impact is equal to $100*100.000 = $10.000.000

As for the probability: according to AHA (2017), there are 5564 registered hospitals in the US. There are 1549 different medical facilities in our dataset. Using this, the probability of a medical facility being attacked is calculated to be 1549/5564 = 0.278 (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. A conservative estimate for that probability would be 0.2, resulting in ALE_o = \$10.000.000 * 0.2 = \$2.000.000.

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 also steal the decryption key 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 normally distributed with a mean of 30% and a standard deviation of 10%.

This reduces the impact to \$10.000.000 * 0.2 = \$2.000.000, resulting in ALE_s = \$2.000.000 * 0.2 = \$400.000.

The ROSI can now be calculated as follows:

$$ROSI = \frac{\$2.000.000 - \$400.000 - \$40.000}{\$40.000} = \frac{\$1.560.000}{\$40.000} = 39 = 3900\ \%$$

References

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

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

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

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