

|  |  |
| --- | --- |
|  |  |
| **Subject Name:** | Social and Professional Issues |
| **Subject Code:** | BTIS3053 |

**Report Title:** Case Study for Professional Issue

**By**

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name:** | | Lam Wei Chun |  |
| **Student ID:** | | B180279C |  |
| **Class ID:** | | BoSE18-C2 |  |
|  |

|  |  |
| --- | --- |
| **Lecturer Name:** | Dr. Lee Huah |
| **Submit Date:** | 24th August 2020 |

Department of Computer Science

**Table of Contents**

[**1.** **Repertoire of Fact** 4](#_Toc47000024)

[**1.1.** **Case Story** 4](#_Toc47000025)

[**1.2.** **The Facts of Case** 5](#_Toc47000026)

[**1.2.1.** **Fact 1: Scenario** (Medical staff accidentally clicked on an email with a virus.) 5](#_Toc47000027)

[**1.2.2.** **Fact 2: Scenario** (Ransomware demands ransom from hospital.) 5](#_Toc47000028)

[**1.2.3.** **Fact 3: Scenario** (The hospital paid the corresponding ransom for the ransomware) 5](#_Toc47000029)

[**1.3.** **Central Ethical Issues** 6](#_Toc47000030)

[**1.3.1.** **Ethical issue 1: Arguments conduct** (The hospital did not conduct email checks.) 6](#_Toc47000031)

[**1.3.2.** **Ethical issue 2: Arguments conduct** (The hospital does not backup any store patient data.) 6](#_Toc47000032)

[**1.3.3.** **Ethical issue 3: Arguments conduct** (Pay ransom to ransomware) 6](#_Toc47000033)

[**2.** **Proposed Appropriate Solutions** 7](#_Toc47000034)

[**2.1** **Duties Perspective** 7](#_Toc47000035)

[**2.2** **Rights Perspective** 7](#_Toc47000036)

[**2.3** **Consequences Perspective** 7](#_Toc47000037)

[**2.4** **Virtues Perspective** 7](#_Toc47000038)

[**3.** **Develop an ethical analysis with theory or theories** 8](#_Toc47000039)

[**3.1.** **Kantian Evaluation** 8](#_Toc47000040)

[**3.1.1.** **Evaluation:** 8](#_Toc47000041)

[**3.1.2.** **Case for:** 8](#_Toc47000042)

[**3.1.3.** **Case against:** 8](#_Toc47000043)

[**3.2.** **Social Contract Theory** 9](#_Toc47000044)

[**3.2.1.** **Evaluation:** 9](#_Toc47000045)

[**3.2.2.** **Case for:** 9](#_Toc47000046)

[**3.2.3.** **Case against:** 9](#_Toc47000047)

[**3.3.** **Rule Utilitarianism** 10](#_Toc47000048)

[**3.3.1.** **Evaluation:** 10](#_Toc47000049)

[**3.3.2.** **Case for:** 10](#_Toc47000050)

[**3.3.3.** **Case against:** 10](#_Toc47000051)

[**3.4.** **Act Utilitarianisms** 11](#_Toc47000052)

[**3.4.1.** **Evaluation:** 11](#_Toc47000053)

[**3.4.2.** **Case for:** 11](#_Toc47000054)

[**3.4.3.** **Case against:** 12](#_Toc47000055)

[**3.5.** **Virtue Theory** 12](#_Toc47000056)

[**3.5.1.** **Evaluation:** 12](#_Toc47000057)

[**3.5.2.** **Case for:** 12](#_Toc47000058)

[**3.5.3.** **Case against:** 12](#_Toc47000059)

[**4.** **Reflections** 13](#_Toc47000060)

[**4.1.** **Reflection on solution.** 13](#_Toc47000061)

[**4.2.** **Reflection on what you learn** 13](#_Toc47000062)

[**4.3.** **Recommendation for Situation Improvement** 14](#_Toc47000063)

[**5.** **Reference** 14](#_Toc47000064)

# **Repertoire of Fact**

A medical centre compromised with ransomware and paid the corresponding ransom. The main reason for paying the ransom is that medical staff cannot access the patient’s medical history, nor can they share X-rays, CT scans and other medical examinations. Because of this, some patients were transferred to nearby hospitals, and the staff had to resort to pen and paper patient admissions and other record keeping. However, paying the ransom to the ransomware will cause those bandits to be more rampant and more active in carrying out these blackmail incidents. If they do not recover in time, this can cause serious problems such as aggravation of the patient's illness or even death.

## **Case Story**

Hollywood Presbyterian Medical Center is a general medical and surgical hospital that originally opened in 1924 as Hollywood Hospital. According to the data at the time, this hospital had 424 beds, more than 500 doctors, and had seen approximately 16,000 patients within a year.

According to a report in Wired Magazine, the hospital’s computer system was attacked by a ransomware virus called Locky, which locks the user out. Thereafter, unless a ransom is paid, the decryption key will not be sent. The ransomware is spread through malicious Word documents masquerading as invoices, so the attack is likely to be a fraud that occurred when an employee mistakenly clicked an email attachment that was actually a phishing.

In the end, the hospital was forced to pay a ransom of about 40 bitcoins (approximately US$17,000) with nothing to do. So that the system returns to normal. When the system returned to normal, the hospital immediately tested all the systems and removed their malware. However, because of this factor, ransomware may begin to actively attack medical establishments and some data-based companies frequently. The reason is because they will pay the ransom if they have nothing to do.

## **The Facts of Case**

Ransomware is that hijacks a computer or data in exchange for money. It can block the data in the computer and ask the victim to pay the corresponding price in exchange for the key to unblock it. Their usual target is still hospitals, other medical facilities or other data-based companies.

### **Fact 1: Scenario** (Medical staff accidentally clicked on an email with a virus.)

Since President and CEO Allen Stefanek stated that the attacks were random, while Symantec stated that Locky was usually spread through malicious Word documents disguised as invoices, the attacks were most likely due to employees A scam occurred by mistakenly clicking an email attachment that was actually a phishing.

### **Fact 2: Scenario** (Ransomware demands ransom from hospital.)

When hospital data is blocked, they cannot access the Internet, nor can they access the patient’s medical history, nor can they share X-rays, CT scans and other medical examinations. Later, they found out that pay the 40 bitcoins (approximately US$17,000) were written on a document in exchange for the decryption key to open the computer data.

### **Fact 3: Scenario** (The hospital paid the corresponding ransom for the ransomware)

The hospital really couldn't find a way to lift the blockade. In the end, the hospital decided to pay the corresponding ransom in exchange for the decryption key. When the hospital successfully unblocked the blockade, it immediately carried out a comprehensive test to remove the malware from all systems, and restored all services ten days after the attack.

## **Central Ethical Issues**

The scope and methods of ransomware attacks are vast and random. In these attacks, victims will certainly appear. Of course, not all victims need to pay the ransom or deal with this problem. However, when someone pays the ransom, it can cause even bigger problems. Although, this is the consequence that the victim must bear.

### **Ethical issue 1: Arguments conduct** (The hospital did not conduct email checks.)

Hospitals should conduct email audits to avoid the invasion of these virus software. Medical staff should not open unchecked emails indiscriminately. Clicking randomly on unreview emails is foolish and reckless, because it is not considered for patients. If an aggression occurs, it may lead to serious consequences.

### **Ethical issue 2: Arguments conduct** (The hospital does not backup any store patient data.)

The hospital should store another backup for emergency situations. If the hospital has backup another copy of data, it would not need to pay a ransom for the ransomware. This behavior was not considered for the patient at all, and there was no sense of responsibility at all.

### **Ethical issue 3: Arguments conduct** (Pay ransom to ransomware)

The hospital couldn't find any way to lift the blockade, and decided to pay the ransomware. This behavior may cause bigger problems, because when the blackmailer successfully ransoms the ransom, he will start to actively attack the relevant units to obtain more ransom. According to data, after the incident, emails from ransomware have skyrocketed recently. This led to a rapid increase in victims.

# **Proposed Appropriate Solutions**

All victims of ransomware face several major problems. Such as how the incident happened, why the incident happened to us and how to solve existing problems. Ransomware seeks to obtain a ransom from the victim in order to obtain benefits. If every victim pays a ransom for the ransomware, this would be an improper way to solve this problem. Therefore, we must resolve such incidents with ethics.

## **Duties Perspective**

The hospital should have some backup to deal with and deal with those emergencies. If the hospital has a backup, then they don’t need to worry about the harm caused by the ransomware. Furthermore, hospitals should not pay ransomware for ransomware. The hospital should look for professionals in the field to deal with the problem. The hospital should have a system function to detect whether there are viruses in the e-mails, and all e-mails that are suspected to be problematic will be regarded as spam.

## **Rights Perspective**

The hospital has the right to decide and implement how to solve the problem, but paying the ransom is definitely not the first choice. The patient has the right to decide whether to stay in the hospital or transfer, because the hospital is not responsible for the patient's information. When a case occurs, the patient has the right to ask the hospital to compensate for a certain amount of loss.

## **Consequences Perspective**

In this case, the hospital paid a ransom for the ransomware, which may cause more serious consequences. For example, when criminals get profits from ransomware, they will be more active in implementing more ransom cases, and they will target other hospitals and medical establishments. When the data in the hospital is blocked, if a patient urgently needs to perform treatment based on the data, this may lead to very serious problems such as aggravation of the patient's condition and even death. Hospitals will also lose the trust of some patients.

## **Virtues Perspective**

The hospital's behavior is irresponsible because there is no backup of any patient data, so there is no way to treat the patient when the incident occurs. In addition, the hospital decided to pay the ransom for the ransomware. This behavior is reckless, but it does not mean it is wrong. After all, they must prioritize the patient's situation. However, this may still cause greater consequences.

# **Develop an ethical analysis with theory or theories**

Apply ethical ideas and principles to evaluate the options and select or defend the one that is best. I will discuss about our duty and responsibility, but desire.

## **Kantian Evaluation**

We could try to imagine that if everyone follows the rule all the time without producing a logical contradiction that undermines the rule at any time. The rule also doesn’t treat others as a stepping stone such as using others to achieve own goals, which means that it doesn’t harm others.

### **Evaluation:**

Based on Kantian theory, people should not pay a ransom for those ransomware. This is because this action violates the rule of moral or universal moral rule. However, in this case, the Hollywood Presbyterian Medical Center paid a ransom for the ransomware, so it came to unlock the blocked data. Based on Kantian theory, this medical center is doing something wrong. the center not only fails to follow the rules that everyone follows, but also hurt others.

### **Case for:**

Paying a ransom for the ransomware will lead the offender to gain benefits in this regard, which is likely to make him more active in the implementation of ransomware. At that time, this will likely harm more people, especially medical equipment and medical places, etc. will be targeted.

### **Case against:**

The Hollywood Presbyterian Medical Center should not pay a ransom to ransomware. They should find professionals to crack this blocked data. This may take a lot of time, but it can make ransomware opportunities fail. During this cracking period, the medical center can move more serious patients to other hospitals, and relatively mild patients can use paper documents to store their information. This may cause losses, but it will effectively avoid more serious problems and the increase of ransomware.

## **Social Contract Theory**

People live together in society according to established ethics and laws. Rational people will abide by this rule because of the resulting benefits to society. Social contracts can be explicit, such as laws, or implicit, such as raising one’s hand in class to speck.

### **Evaluation:**

From the perspective of social contract theory, we should consider the rights of the Hollywood Presbyterian Medical Center. When they are attacked by ransomware, they must quickly decide how to deal with the problem. In the end, they chose to pay ransom to ransomware, but this was inconsistent with social contract theory, because their choice brought adverse effects to society, such as an increase in ransomware cases.

### **Case for:**

The behavior of the Hollywood Presbyterian Medical Center is selfish, because while protecting its own interests, it requires most of the consequences borne by others, and others may become victims of timid cybercriminals.

### **Case against:**

Although, the Hollywood Presbyterian Medical Center has the right to decide how to deal with ransomware issues. However, their choices cause social harm. Therefore, they should whether their choice will have serious consequences for society or others.

## **Rule Utilitarianism**

This theory can be understood as everyone follows this rule because its affect is always the greatest increase in the total good. In other words, if the greatest increase in the total good of an action is long-term, then this action is correct.

### **Evaluation:**

The medical center paid a ransom for the ransomware to solve the problem of blocked data, so that the medical center can continue to perform daily. But this solution may cause greater and more serious harm, because the offender feels that they can profit from it, so the solution is not ideal and justified.

### **Case for:**

After paying the ransom, there will be no major problems at the moment, but maybe in a few months, ransomware incidents will increase greatly. Because the perpetrators also profit from ransomware as before. When the offender succeeds once, he will feel that he will succeed the second, third times and more, which leads to a large increase in emails from ransomware. In addition, the target will focus on medical alms and medical places.

### **Case against:**

According to this theory, the medical center should not use this method to solve the ransomware problem. This method will only allow you to solve current problems, which may cause more serious damage to other medical center or hospital.

## **Act Utilitarianisms**

In result in the maximum net increase in the total good of the affected parties.

### **Evaluation:**

To analysis this case by act utilitarianism, the affected parties and the effects of the other parties after the ransom is paid. The measurement units used in this analysis are "happiness" and "happiness", and the sum and subtraction of numbers indicate their increase or decrease. Affected parties including medical center, patients and other medical center or hospital. The Hollywood Presbyterian Medical Center paid a ransom to the ransomware, so that their computer system can operate normally, hospitals and medical staff can continue to use the system, making them feel happy, no need to use paper documents and can continue to make money. In this regard, we can add the mark +20 to the Medical center of actions and decision. In addition, when the computer system is used, the patients in the Medical Center can get more proper and accurate treatment. In this regard, we can add +5 to the mark. However, paying the ransom to the ransomware may cause more crime. This may cause the perpetrators to actively mass-produce ransomware, resulting in a large number of victims, so we need reduce mark -15 to the consequences of paying the ransomware.

In conclude of analysis, we found that the benefits (happiness of people) of paying the ransom to the ransomware is outweighing of the harm (unhappiness of people). So, the action of Medical center was doing right in act utilitarianism.

### **Case for:**

From act utilitarianism, it is only focuses on the most benefits or goods or happiness of the affected parties. Even the consequence of the action is breaking the rule such as lying in specific situation to solve the problem. The right action is depending on how much benefits it can be gained and not involved and affected by the moral rule.

So, Medical Center pay the ransom to the ransomware that may cause the ransomware of victims of future to increase but the overall of benefit in this case is greater than a part of it. Therefore, the medical center’s action is determined as a right action.

### **Case against:**

In this cases, we only can do an assumption to every case and the effect to the affected parties. Also, to calculate the utility accurately have to spend a lot of time and energy to analysis every possible decision and consequence to case. So, we just assume a simple and clear of possible case happened to do the analysis.

## **Virtue Theory**

Virtue Ethics (or Virtue Theory) is an approach to ethics that emphasizes an individual’s character as the key element of ethical thinking, rather that rules about the acts themselves (Deontology) or their consequences (Consequentialism).

### **Evaluation:**

By the analysis of virtue theory, Hollywood Presbyterian Medical Center is irresponsible, because they decided to pay the ransom for the ransomware, and did not consider other companies and medical establishments. After all, this behavior may cause ransomware to attack these related parties frantically. The medical center should look for some experts in this area to help solve the ransomware, rather than compromise with the ransomware.

From above analysis, Medical center was wrong to pay the ransom to the ransomware.

### **Case for:**

By the virtue ethics, it is simpler to determine whether the case is right or wrong, the one who break the moral rule and perform the right action or right character is determined as wrong action to virtue ethics. According to the simple rule of virtue ethics, Medical Center is performing irresponsible action in the case, so we can result that Medical Center was wrong in virtue ethics analysis.

### **Case against:**

Even the case shown that Medical Center pay the ransom is wrong action, but on other sides of consequence, the non-payment of the ransom by the medical center may cause the medical center to be unable to perform daily work, and the medical center will suffer huge losses, and may even lead to aggravation or death of the patient. This may cause another morally wrong action.

# **Reflections**

# **Reflection on solution.**

By analyzing many workable ethical, most ethical theories believe that the behavior of medical centers is morally wrong, because the harmful consequences of such behavior exceed all benefits. Hollywood Presbyterian Medical Center should not have pay the ransom to the ransomware instead it should have consult experts in related fields and ask them to help solve the ransomware. By paying a ransom to give ransomware, the blocked data can be opened. The Hollywood Presbyterian Medical Center could have looked for experts in related fields for advice in order to resolve the ransomware. This may take a long time, but the medical center is still capable of handling things during this maintenance period. During this period, medical staff can use paper documents to store patient information. More serious patients can be transferred to the hospital. Although this may cause a greater loss, it will not allow the criminals to benefit from the ransomware. After all, this will make them more active in implementing more ransomware, and the targets will be defined in medical equipment and places.

# **Reflection on what you learn**

There are a lot of consequences with regards to the pay the ransom to the ransomware which are both negative and positive. Therefore, I hope that this case serves as a lesson for people to learn from on how to handle and how not to handle a situation. Below are some lessons I have learnt:

**Lesson learnt from draft of topic planning**

I learned that each theory gives us different views on the same issue, which means that each theory produces different opinions. To fully understand these theories requires in-depth understanding. By doing this, we can choose the most morally correct actions suggested by these feasible theories.

**Lesson learnt from process of assignment work**

Every action we choose to take has consequences. Each theory can help us analyse the consequences of our actions. We must analyse each action to understand the consequences of these actions and whether we can afford it. Therefore, if I encounter such a problem in the future, I will definitely use these workable theories to take correct actions.

**Lesson learnt from review of issues and need achieved**

In many cases, this is correct for us but may not be correct for others. Or it is wrong now, but it is correct in the long term. In so many situations, how should we define it? Therefore, by implementing all these workable theories, people can follow whether he did it right or wrong. I learned that the corresponding workable theory should be used to analyse whether this behaviour is right or wrong.

# **Recommendation for Situation Improvement**

In my opinion, the Hollywood Presbyterian Medical Center should consult with experts in the ransomware case and ask them for help. They should analyze the feasible theories and get the corresponding consequence analysis before deciding how to deal with the problem. Medical staff should patiently use paper documents to handle affairs, instead of putting pressure on the medical center to quickly restore data, etc. After being attacked, the medical center should immediately notify other parties in the field and notify them that they will pay the ransom to the ransomware. Let them take action to do some preventive measures such as backing up data and so on.

# **References**

1. infosecinstitute. (2020). *infosecinstitute*. Retrieved from Ransomware Case Studies: Hollywood Presbyterian & The Ottawa Hospital: https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/ransomware-case-studies-hollywood-presbyterian-and-the-ottawa-hospital/#gref
2. The Conversation. (2020). *The Conversation*. Retrieved from When it comes to ransomware, it’s sometimes best to pay up: https://theconversation.com/when-it-comes-to-ransomware-its-sometimes-best-to-pay-up-78036