CYB E 2340 Ethical Dilemma

Nina Gadelha

Almost four years ago, cybersecurity was faced with a tough ethical dilemma. In May of 2021, a South American based meat-packing company, JBS, was attacked by a group of cyber criminals. These hackers used a series of ransomware attacks to shut down operations in Australia, Canada and the United States. These attacks disrupted their business operations and threatened their food supply chain [1]. JBS had to act quickly, as their company deals with various types of meats, which do not have an extensive shelf life. The attackers offered JBS a retraction of their ransomware, in exchange for eleven million dollars. Although the JBS cybersecurity team did attempt to restore their operations themselves, they were not able to do so in a timely manner. Ultimately, JBS ended up striking a deal with the attackers. After they were able to regain control of the systems, they wired 11 million dollars to the attackers through bitcoin. JBS stated that it was a difficult decision, but they ultimately believed that it was the best way to quickly restore operations and protect their supply chain, employees and customers [2].

I believe this situation is classed as an ethical dilemma rather than a decision, due to the fact that the outcome choice could be different, for many different reasons, based on who had to make it. For example, the CEO, Andre Nogueira, believed the best choice was to pay eleven million dollars, in order to protect company and customer data, and prevent further disruptions/data leaks [2]. However, the FBI discourages companies from paying ransoms. Perhaps if JBS was a United States based company, they wouldn't have been allowed, or strongly discouraged from paying the attackers. Different individuals, cultural perspectives and levels of expertise could all influence how this decision is approached, leading to varying conclusions on the most ethical course of action.

This outcome would have been much different, if this company approached the decision making through a Kantian perspective. Kantianism, emphasising logic and duty regardless of consequences, would deem paying the attackers to be unethical. Even though customer's data could've been compromised and company value would have decreased, JBS should not have paid the group of hackers, in a Kantist's mind. Kantian ethics discourages anyone from engaging in actions that could not be universally applied as moral law [6]. Paying the ransom would be considered unethical, as it violates categorical imperative, which demands that actions be guided by universal moral laws [6]. If all companies paid ransoms, ransomware attacks would become more common, incentivizing criminal behavior [7]. Kantian ethics also requires treating individuals as ends in themselves, not as means to an end. Engaging with the attackers, who are violating moral law (by conducting the attacks), contradicts Kant's principle of humanity [3]. The duty to uphold justice and not support/incentivize criminal activities

would obligate organizations to refuse payment, regardless of the negative outcome it could have on the company, employees and customers.

However, not all ethical theories disagree with the decision made by Andre Nogueira. I believe someone with a Utilitarian perspective would've come to the same conclusion as JBS. Utilitarianism emphasizes maximizing overall happiness and well being [6]. Taking that into consideration, paying the ransomware would've maximized happiness for customers and potentially employees (and attackers but not sure if that's relevant here). Customers would be satisfied that their data wasn't leaked and they could get their product, since operations would be successfully running after the ransom was paid. Employees would be relieved that their company was up and running again, allowing them to keep their jobs and also keeping their own sensitive information private. Although the company would've taken a hit after paying eleven million dollars, they would be able to continue their business and gain approval from customers, as they chose to protect them and their information. Since paying the ransom would result in the swift restoration of operations, financial stability for employees and customer trust, a Utilitarian would likely view it as the morally correct choice [7].

Although I do personally believe a Utilitarian perspective would've led them to the same conclusion as JBS, it is worth mentioning that it could depend on the type of Utilitarianism. Rule Utilitarianism would argue that paying the ransom could set a precedent that ultimately harms more people over time (similar to the Kantianism argument that it could incentivize attackers to continue ransomware attacks) [4]. Act Utilitarianism, which is what was talked about in the paragraph above, would support then ransom being paid, as for that specific situation, it would benefit the most people (customers, employees and business).

A virtue ethics perspective is harder to analyze, as both outcomes can be concluded based on the virtue ethics 'guidelines/values' [7]. Virtue ethics is based on being good, which emphasizes character and virtues, advocating for actions that reflect moral excellence. Virtue ethics emphasizes virtues such as justice, courage, honesty and prudence [6]. Nogueira's action to pay the ransom could have been seen as an act of prudence, since he considered the well-being of customers, employees and the company's long term stability. By this logic, virtue ethics could have supported the decision he made to pay the attackers.

However, we can also conclude the opposite outcome, while still basing our reasoning around virtue ethics. Paying the attackers would be an act that lacks moral courage and justice, as it rewards unethical behavior. Deciding based on these specific virtue ethic values, would lead one to conclude that paying the ransom would be unethical, and therefore the wrong choice.

The conclusion is drawn based on what kind of leader one should strive to be (based on virtue ethics) in such a situation [5]. A leader who values wisdom and responsibility, could justify making the

payment, while an individual who prioritizes courage and justice would refuse to interact with the hackers.

I would argue that none of these perspectives agree on the choice, even if they come to the same conclusion. A Kantist should easily conclude that not paying the criminals is the right decision, due to their duty to be consistent with moral law, and it is not morally right to interact with those causing harm to others. Someone with a Utilitarian perspective would reason that the correct act would be to pay the attackers, as that outcome results in the least damage done to other people. An individual who practices virtue ethics, would be at somewhat of a crossroads. They could justify both conclusions, so it ultimately depends on what virtues the specific person values more. Overall, even if two of the perspectives draw the same conclusion, it would be hard to say they agree, due to their reasoning being different and the 'ease' of choice.

Ultimately, I personally would conclude that paying the ransom would be the best choice. I would conclude this based on Utilitarian perspective and reason. I do believe that to keep the trust and loyalty of the employees and customers, one should pay the money in order to keep their sensitive information/data safe. I would also conclude that paying the money would result in well-being kept for the most amount of people (for this specific situation). Company employees would be able to keep their job, the customer's information would be safe and customers/distributors would continue to receive our product, that they could then sell to keep their own business afloat. If I risked not paying the attackers, the entire company could collapse. Not only would immediate employees be out of a job, it could also impact distributors the company sells to. Customer's private information would be exposed, and it would be hard to come back from a deficit/reputation like someone would gain from this situation. Coming to a conclusion in this situation is very difficult, I'm not sure if there is a 'right' answer. Based on an individual's experiences, values and understanding, different conclusions could be drawn by many different reasons/justifications [7].

Although I have my personal opinions, I do see how others could disagree with my answer and justification behind it. Why would you ever pay someone who has caused great harm to your business, customers and employees? Why would you ever incentivize unethical behaviour, increasing the likelihood of it happening in the future? Wouldn't this situation 'inspire' and encourage future hackers to execute a similar plan, as they have seen success from other groups? I understand, and respect, how some people would be willing to let their business crumble, just to uphold what they believe is ethically correct. I also generally agree that unethical behaviour should not be tolerated or rewarded. However, I say generally because there are some situations, such as this one, where I believe for the greater good, payment in order to restore normally, can be considered.

This is similar to our in class discussion on if whistleblowers are considered unethical or heroes, and if we should arrest or financially compensate them [7]. Although I generally wouldn't 'support' whistleblowing, I can recognize that in certain situations in which doing the action would cause an overall net benefit to a large number of people, it can go unpunished and in rare cases, even lead to rewards. Like this JBS situation, the decision would have to be made based on how many people it would 'save' vs harm. Speaking from a true Utilitarianism perspective, if it is for the greater good of more people, I would argue that tolerance and payment can be justified.

The consideration of customers, employees, distributors, the CEO and their family, would ultimately lead me to the conclusion that paying the ransom would lead to the overall benefit of most groups, relating to this specific scenario. This situation is a very challenging and likely, an ethical dilemma that could be faced by many companies all around the world. The 'solution' and justification behind it is very unique, as it seems there is no universally correct answer, and it all depends on the person you are, and what you value.

Works Cited

[1] Collier, Kevin. “Meat Supplier JBS Paid Ransomware Hackers $11 Million.” *CNBC*, CNBC, 10 June 2021, www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html?msockid=04fe476178c06f0608b7532d794e6e9a.

[2] Durbin, Dee-Ann. “Meat Company JBS Confirms It Paid $11m Ransom in Cyberattack.” *AP News*, AP News, 10 June 2021, apnews.com/article/europe-hacking-technology-business-353f8dea34bbbba15207ff350e7a2f0f.

[3] Johnson, Robert, and Adam Cureton. “Kant’s Moral Philosophy.” *Stanford Encyclopedia of Philosophy*, Stanford University, 21 Jan. 2022, plato.stanford.edu/entries/kant-moral/.

[4] Sinnott-Armstrong, Walter. “Consequentialism.” *Stanford Encyclopedia of Philosophy*, Stanford University, 4 Oct. 2023, plato.stanford.edu/entries/consequentialism/.

[5] Hursthouse, Rosalind, and Glen Pettigrove. “Virtue Ethics.” *Stanford Encyclopedia of Philosophy*, Stanford University, 11 Oct. 2022, plato.stanford.edu/entries/ethics-virtue/.

[6] Ideas from lectures

[7] Ideas from in class discussions