Ethan Roepke

CPRE 2340: Assignment 2

Cybersecurity professionals encounter ethical dilemmas all the time, and it is not always clear what course of action to take immediately. A recent example that involved an ethical dilemma was surrounded by ransomware attacks on a healthcare institution in October 2023. A major hospital system in the United States was targeted by a ransomware attack, destroying patient care systems, delaying surgeries, and putting lives at risk. The group of attackers demanded a multimillion-dollar ransom in cryptocurrency. In exchange for the money, they would restore all of the hospital operations. The cybersecurity team at the hospital was in a difficult position during this attack. The team had to decide if they should advise hospital leadership to pay the ransom and restore operations quickly or refuse to pay and put many lives at risk. Following the government guidelines, organizations are generally advised to refuse to pay, but this may delay addressing patient suffering and even lead to a loss of life.

This example presents no clear right answer and requires an analysis from multiple perspectives. We will be applying Kantian ethics, Utilitarianism, and Virtue Ethics to understand what the right thing to do might be. Each of these ethical frameworks provides a unique lens through which to evaluate the decision, allowing professionals to explore the broader implications of their actions. Balancing moral principles, long-term consequences, and character-driven considerations is a daunting task in high-pressure situations like these.

Immanuel Kant’s ethical framework suggests that actions are judged based on adherence to moral duties rather than consequences. Using Kantian perspective for the hospital system attack, paying the ransom would be the wrong decision because it would be supporting criminal activity and violating universal moral laws. Kant’s perspective is that if every organization paid ransoms to attackers, then cybercriminals would be determined to continue attacks. This leads to a cycle of harm for patients and benefits the attackers if they get paid for every attack. The cybersecurity team should refuse to pay even if it results in longer disruptions to patient care. The emphasis on universal principles and the need to avoid condoning unethical behavior underscores why Kantian ethics would denounce payment, regardless of immediate suffering.

Utilitarianism, on the other hand, focuses on maximizing the overall happiness of society and minimizing harm. For the hospital system attack, the decision should be based on which action produces the greatest net benefit for all participants. If paying the ransom allows hospital operations to resume quickly, saving lives and reducing patient suffering, then utilitarianism would favor paying the ransom. However, from a future-oriented perspective, paying the ransom might push cybercriminals to conduct more attacks. If attackers see that they can profit from such actions, more attacks will occur, leading to greater overall harm. The short-term benefits of restored medical services must be weighed against the long-term risks of incentivizing criminal activity.

A potential agreement could be negotiated with law enforcement and cybersecurity agencies to track the attackers while the company prepares for alternative recovery solutions. Engaging all stakeholders and leveraging specialized resources could enable a more nuanced approach to the dilemma. If a workaround is available, refusing to pay could ultimately be the better long-term utilitarian choice, emphasizing the importance of systemic resilience.

Virtue ethics evaluates actions based on moral character and the virtues they promote. In the hospital system attack, the key virtues in question include courage, justice, and prudence. A virtuous cybersecurity professional would likely consider what a responsible and ethical leader should do. Courage might mean resisting the temptation to take the easier route and not pay the ransomware. They would instead work toward a lawful and sustainable solution. Justice demands that criminal acts not be rewarded, reinforcing the importance of standing firm against cyber threats. Prudence requires balancing idealism with real-world consequences, which include potential loss of life. This framework encourages professionals to think about their role in creating a secure digital landscape and the example they set for others in the industry.

From the virtue perspective, the decision centers on the professional's commitment to fostering a secure and ethical cybersecurity environment. A virtue ethicist might favor refusing payment but would also encourage immediate solutions to restore hospital operations, such as employing robust backup systems or seeking assistance from federal agencies. The emphasis here is on upholding values and demonstrating leadership, even in the face of immense pressure.

Kantian and Virtue Ethics lean toward refusing to pay the ransom, while Utilitarianism leans toward payment being justified if it results in significantly reduced harm. The disagreement begins because Kantian and virtue-based approaches prioritize moral principles and character integrity, while utilitarianism prioritizes outcomes and consequences. Each perspective provides valuable insights, but the ethical tension remains unresolved. This underscores the complexity of decision-making in cybersecurity, where professionals are often forced to navigate conflicting priorities under intense scrutiny.

This separation highlights an ethical tension in cybersecurity. As professionals, we must ask whether decisions should be made based on strict moral duties or whether potential consequences should dictate the course of action. Cybersecurity professionals must balance these considerations under intense pressure. The weight of these ethical dilemmas highlights the need for a well-trained, ethical workforce that can respond swiftly and decisively when faced with such challenges. It also raises questions about the broader societal impacts of paying ransoms and how the industry can collectively address this growing threat.

If I were in the chair during the hospital system attack, I would resist paying the ransom and instead focus on alternative recovery efforts. Paying would be a last resort if I am unable to find another recovery option for the hospital. I can see others going against me and advocating for paying the ransom to protect patients' health, implying a utilitarian perspective. However, I am thinking about the future and how paying ransom multiple times increases harm. Building a strong culture of prevention and preparedness is crucial to avoiding such dilemmas in the first place.

The ethical dilemma of whether to pay a ransomware demand in a healthcare environment demonstrates the complexity of cybersecurity decision-making. Kantian and virtue ethics argue against payment due to moral duty and character considerations. Utilitarianism allows for payment if it minimizes harm. In real-world practice, cybersecurity professionals must weigh ethical principles against practical consequences. This makes for split-second decisions with deep consequences. This case highlights the importance of proactive cybersecurity measures, ethical training, and crisis preparedness in mitigating ethical dilemmas before they arise. Additionally, fostering an environment where ethical principles are part of everyday decision-making can help reduce the emotional and moral burden during crises, ensuring that teams are better equipped to make sound judgments.