In an article by Matt Mathias titled "Sticky fingers – Cyber security expert weighs in on Welch's online extortion," the cyber-attack targeting Welch's is discussed. It reveals that a criminal group is taking credit for the attack and is demanding ransom from the company. The incident has disrupted Welch's operations, prompting the gradual return of employees and the restart of production lines. Threats to release sensitive information if the ransom isn't paid have been made by the attackers. A dark web search unveiled a post claiming to contain confidential data from Welch's, though the company has yet to confirm the ransom amount or the validity of this claim. Cybersecurity experts warn of the repercussions of stolen information being traded on the dark web, including identity theft and financial fraud. The attack displays the necessity for string cybersecurity measures such as encrypted backups and regular screenings. While Welch's is actively working to mitigate the attack's impact, specifics regarding their response to the extortion attempt remain undisclosed.

The cyber-attack and extortion attempt not only disrupt the operations of Welch's, but also directly impact the employees and the farming families who own the cooperative. Because Kantian ethics emphasize the inherent worth and dignity of individuals, Kant would argue that these individuals deserve respect and should not be treated as a means to an end for financial gain for the criminal group. Kantians also emphasize the importance of acting in a way that respects the rights and well-being of others. Welch's has a duty to protect its employees, customers, and stakeholders, including the potential consequences of cyber-attacks. This duty extends beyond mere compliance with legal obligations to actively safeguarding against foreseeable risks. Finally, Kant's categorical imperative requires that actions could be consistently applied without contradiction. In this case, if Welch's were to comply with the extortion demands, it would set a precedent that could encourage further attacks and extortion

attempts. From a Kantian perspective, Welch's must consider whether their actions, such as paying the ransom, could be morally justified if everyone were to act in the same way.

Utilitarians would primarily consider the consequences of Welch's actions in response to the cyber-attack and extortion attempt. They would advocate for actions that minimize overall harm and maximize well-being. Welch's must assess whether paying the ransom or refusing to pay would lead to greater harm. For example, if paying the ransom would prevent further disruption to operations and protect sensitive information from being leaked, it might be justified if the harm caused by the cyber-attack outweighs the harm caused by rewarding criminal behavior. Utilitarians would also consider the interests and well-being of all stakeholders involved, including employees, customers, shareholders, and the broader community. Welch's must weigh the potential impact of their decisions on each group and strive to maximize overall happiness. Finally, Utilitarians would support investing in preventative measures and preparedness to mitigate the risk of future cyber-attacks. By implementing stronger cybersecurity protocols, encryption measures, and employee training programs, Welch's can reduce the likelihood and severity of future attacks, thereby maximizing overall happiness by safeguarding against harm.

Virtue ethics emphasizes the development of moral character and virtues such as honesty, integrity, prudence, and courage. Welch's response to the attack and extortion attempt would be evaluated based on whether the company demonstrates these virtues in its actions and decisions. Virtue ethics also considers the well-being of employees and stakeholders as integral to ethical decision-making. Welch's would be expected to demonstrate virtues such as compassion, care, and fairness in its efforts to protect the interests and livelihoods of its employees affected by the attack. This might involve providing support, resources, and assistance to affected individuals and their families. Finally, Virtue ethics places importance on the virtues of trustworthiness and

reliability in interpersonal relationships and organizational conduct. Welch's would be evaluated based on whether it maintains the trust of its employees, customers, and stakeholders by acting in accordance with virtuous principles and fulfilling its commitments.

While the Kantian, utilitarian, and virtue perspectives each provide different frameworks for ethical decision-making, they ultimately agree that, in this scenario, refusing to pay the ransom is the most ethical course of action. All three perspectives prioritize principles such as honesty, integrity, and the greater good, which are compromised by negotiating with criminals. Additionally, paying the ransom could have negative consequences in the long term, such as encouraging further attacks and funding criminal activities. Therefore, the decision not to pay the ransom aligns with the principles of Kantian ethics, the goals of utilitarianism, and the virtues promoted by virtue ethics.

As someone studying cybersecurity, I came to the same conclusion not to pay the ransom based on the ethical frameworks discussed. Prioritizing the long-term security and well-being of employees, customers, and stakeholders, as well as upholding ethical principles such as honesty and integrity, would guide my decision-making process. Additionally, recognizing the potential consequences of paying the ransom reinforces the importance of refusing to negotiate with criminals because, as previously discussed, paying the ransom may embolden cybercriminals to target Welch's again in the future or attract attention from other malicious actors seeking similar payouts.

While the Kantian, Utilitarian, and virtue perspectives all agree it is not a good idea to succumb to ransom demands in cyber-attacks, some individuals might argue that paying the ransom could be the most pragmatic short-term solution for Welch's. Paying the ransom could expedite the recovery process, allowing Welch's to regain access to crucial data and systems

more quickly. This could minimize the overall disruption to their operations and prevent further financial losses. Additionally, If the attackers follow through on their threat to release sensitive information, Welch's could face legal and regulatory repercussions, as well as damage to their brand reputation. Paying the ransom could prevent the exposure of confidential data, safeguarding both the company and its customers, and in some cases, the cost of paying the ransom may be lower than the potential losses incurred from prolonged downtime, data loss, or legal battles. From a purely financial standpoint, paying the ransom could be viewed as the most cost-effective option.