Is it ethical for corporations or municipalities to pay cyber ransoms?

With the transition to stay-at-home work, ransomware has seen an increase in popularity as an attack. In September, Fairfax County schools experienced a ransomware attack, likely spurred by the transition to online learning for the fall semester. They are not alone- a recent study by Check Point Software found that Ransomware attacks were up as much as 50% in the third quarter of 2020 (2).

Thinking about the ethical underpinnings of whether or not to pay, a central emphasis should be placed on the focus of the attacks. Hospital attacks are arguably the most directly dangerous to the individual. They should not be considered the same as business attacks. The American Hospital Association asserts, "Ransomware attacks on hospitals are not white collar crimes, they are threat-to-life crimes because they directly threaten a hospital's ability to provide patient care, which puts patient safety at risk." (4) While business and monetary loss may indirectly threaten the livelihoods of its victims, ransomware attacking hospitals is a direct threat on people's lives.

The ransomware threat to the healthcare sector is not hypothetical either, the Fortune-500 and health care giant United Health Services experienced a significant attack in September 2020, affecting their IT network and records keeping (5). Ransomware has also affected people's care directly: recently, in Germany a homicide investigation was opened about a ransomware attack while a woman was to receive life-saving treatment, forcing her to be redirected to a different hospital, and ultimately leading to her death.(6)

In regards to ethics, Fairfax County Schools had portions of private data released after not paying for the ransom. Not paying for a ransom was justified, as Brent Callow, a threat analyst stated, because paying enabled future attacks and crimes. "These attacks happen for one reason and one reason only: they're profitable," he said. "If the flow of cash stops, the attacks will stop." (1). However, the leak of student and teacher data, while disappointing and potentially harmful, requires different treatment from a hospital system.

Hospital ransomware is particularly difficult because of the danger that not paying might have, as stated above. From a utilitarian perspective, it would seem that paying a cyber ransom, if it would save lives and prevent endangerment to patient care, would be net worthwhile in almost any situation. In the case of a monetary assessment, while monetary bounties have increased, the hospitals' payment of a ransom to cybercriminals likely would be far exceeded by the cost of care, potential loss of data, and obviously, the potential for injury or death if care were altered.

Thinking about a Kantian perspective, I believe that ransom paying should be justified under the theory. If the hospital and patient's ultimate expectation is that the patient should be helped at any cost, this ethical view should supersede the counterargument of future prevention. We could perhaps universalize this rule as allowing payment of bounties in the cases where human lives were put in jeopardy. In Kantianism, people can never be used as a means to an end, and if a hospital did not pay its ransom, in the attempt to stop future attacks, the patient's potentially

compromised care would mean that the patient themself was used as a means to the hope of future attack prevention.

The social contract ethical view would also be complex, as there are competing contracts at work. The hospital and doctor have an obligation to uphold the patient and hospital expectation of an excellent standard of care, but at the same time, they have an obligation to protect the privacy of the doctors and patients within the hospital system. Since, in terms of larger society, we have historically forgone privacy for safety, I would suggest that most would agree that our contract considers safety of greater need than privacy, and could see that a bounty may be justified.

Ultimately, as with the readings and videos, we need new solutions and ideas to counter the growing challenges regarding cyberattacks. In regards to hospitals, the AHA suggests a collaborative effort between hospitals and government in order to fight against future attacks, and that kind of collaboration will be increasingly necessary as we move forward while remaining in a heavily-online work and living situation.

(1) https://www.washingtonpost.com/local/education/hackers-post-stolen-information-from-fairfax-school-district/2020/10/10/edf5f050-0b1a-11eb-859b-f9c27abe638d_story.html
(2) https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/
(3) James A. Sherer, Melinda L. McLellan, Emily R. Fedeles, and Nichole L. Sterling, *Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 Rich. J.L. & Tech. Ann. Survey (2017), http://jolt.richmond.edu/2017/04/30/volume23_annualsurvey_sherer/.
(4) https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed
(5) https://techcrunch.com/2020/09/28/universal-health-services-ransomware/
(6) https://www.bbc.com/news/technology-54204356