This research addresses the ethical dilemma(s) associated with paying attackers during ransomware attacks. The goal is to provide an ethical framework for stakeholders to consider when faced with the decision to pay or not to pay. Existing research focuses on preemptive measures to prevent an attack from occurring; this capstone focuses more closely on reactive measures to assist in the decision-making process for both the government and private sector.

**Problem Statement and Goals**

This research uses consequentialist ethics to determine the ethical permissibility of conceding to ransomware attacks given the following variables:

- Government vs private sector
- Sensitivity of data
- Probability of receiving encryption key
- Ability to pay
- Timeliness of attack
- Form of payment
- Entity paying the ransom
- Number of individuals affected by attack

**Approach**

This research addresses the ethical dilemma(s) associated with paying attackers during ransomware attacks. The goal is to provide an ethical framework for stakeholders to consider when faced with the decision to pay or not to pay. Existing research focuses on preemptive measures to prevent an attack from occurring; this capstone focuses more closely on reactive measures to assist in the decision-making process for both the government and private sector.

**Results**

Simplified flow chart highlighting ethical decision-making process utilizing above variables.

Ultimately, the ethical responsibility is relative to the projected consequences of a decision given specific variables.

Collin Kane
United States Naval Academy