The following section outlines additional arguments in support of HR 215:[3]

Ransomware is a serious and growing threat

Cybercrime is escalating at an unfathomable pace and is costing victims billions of dollars. One of the most concerning areas of cybercrime is ransomware, whereby cyber criminals prevent a victim from accessing their own computer files through encryption until the victim pays a ransom. Losses from ransomware have increased significantly.[4]

Hospitals, school districts, state and local governments, law enforcement agencies, large and small businesses, and individuals have all been targeted by ransomware attacks. The consequences of these types of attacks can be catastrophic. The inability to access important data could mean the cessation of vital services, financial losses, and even death in cases where electronic patient records are encrypted.

Given the serious potential consequences of ransomware attacks, more must be done to deter cyber criminals from launching such attacks.

HB 215 establishes necessary and strong deterrents against the use of ransomware

By explicitly outlawing the possession of ransomware with the intent to use it, HB 215 establishes a strong deterrent against this type of malicious software. HB 215 makes it very clear to cybercriminals that the mere possession of ransomware with the intent to use it is a crime.

Moreover, HB 215 establishes significant penalties for the possession of ransomware which is a strong and effective step towards deterrence.

Explicitly criminalizing the possession of ransomware software provides significant advantages over the current extortion statute

HB215 takes a preventive approach to combat ransomware that offers some distinct advantages over the subsumption or inclusion of ransomware attacks as a form of extortion:

1. By criminalizing the possession of ransomware without research purposes, HB 215 empowers local law enforcement and prosecutors to investigate and prosecute attackers before they act, potentially reducing the risk of harm to public and private cyber-infrastructure.

---

[3] This portion of the testimony was prepared with the helpful assistance of CHHS externs: Oluwatosin Ajayi; Nicky Arenberg Nissin; Benita David-Akoro; and Shravana Sidhu.

[4] FBI, Public Service Announcement, October 2, 2019, available at: https://www.ic3.gov/media/2019/191002.aspx.