and exploited an unpatched system in Medstar Health to deploy the ransomware malware. The ransomware attack on Medstar in 2016, forced 10 hospitals and 250 outpatient centers in the healthcare network to switch to paper, posing a serious threat to patient safety. In addition, Medtsar had to divert patients seeking emergency care away from their facilities, resulting in serious financial losses.[1]

More recently, in December of 2019, hackers used Ryuk, a malicious type of ransomware, to lock up computer data until the target pays for the key to release it. It is estimated that it cost New Orleans about $17 Million to recover.

And let's not forget what happened here in Baltimore MD. In May 2019, hackers used an extremely powerful ransomware called RobinHood, to prevent access to data on the server, demanding payment for the digital key to unlock the data. The encryption algorithms used render it impossible to replicate the key, thus creating a reliance on the hackers to release it. The attack, which brought down Government emails, halted online payments to city departments, and prevented real estate transactions from being processed, debilitated the city for weeks and cost an estimated $18 Million to recover.

According to a study put out by Emisoft, a security and anti-virus company, in 2019, the US faced an "unprecedented and unrelenting barrage of ransomware attacks." The study tallied 103 state and municipal governments and agencies that were hit last year, along with 759 healthcare providers and 86 universities, colleges and school districts nationwide.[2]

Ransomware attacks drain a stupendous amount of time and resources, and hackers have caught on to that. These malicious actors have understood that the value of preventing a disruption of services is often higher than the value of the mined data sold on the dark web. Ransomware attackers have the full intention to cause as much disruption as possible, even at the cost of public safety, for the purpose of financial gain.

Therefore, I am asking you not to wait to be reactive. By the time my consequence management plans need to be activated, it is too late, damage has already been done. By criminalizing the possession of ransomware, HB 215 empowers local law enforcement and prosecutors to investigate and prosecute attackers before they act, potentially reducing the risk of harm to citizens, critical infrastructure, and other private or public organizations.

---

[1] *See* https://healthitsecurity.com/news/medstar-ransomware-attack-caused-by-known-security-flaw

[2] *See* https://www.govtech.com/security/Ransomware-in-New-Orleans-Attack-Is-Likely-Organized-Crime.html