Testimony in Support of HB 215 (2020)
Criminal Law – Crimes Involving Computers – Ransomware
House Judiciary Committee, January 28, 2020

Sponsor: Delegate Erek Barron and Delegate Wanika Fisher

Testimony by: Netta Squires, JD, MSL, CEM

I offer this testimony in support of HB 215 in my personal capacity.

Good Afternoon, Chair Clippinger, Vice Chair Atterbeary, and Members of the Committee,

My name is Netta Squires, I am a Senior Law and Policy Analyst for the Center for Health and Homeland Security at the University of Maryland Carrey School of Law , I am also an Adjunct Professor of Cybersecurity Technology and Digital Forensics at the Graduate School, University of Maryland Global Campus, and Adjunct Professor of Emergency Management at the Mid Atlantic Center for Emergency Management. In addition, I am a Certified Emergency Manager by the International Association of Emergency Management. I have a JD with a focus in Disaster Law, a MSL in Cybersecurity Policy and a Graduate Certificate in Cybersecurity Technology.

My academic and professional background are exactly in the crossroads of fields we are discussing today; law, cybersecurity, and emergency management.

I am here in support of HOUSE BILL 215, Criminal Law- Crimes Involving Computers- Ransomware.

As a Regional Preparedness Specialist for the National Capital Region and a Planner for Montgomery County Office for Emergency Management and Homeland Security, a significant portion of my job entails Consequent Management planning. I.e., what's the plan once something has occurred. This could be providing a shelter following a fire, opening a family reunification center following an active assailant attack, or activating the Cybersecurity Incident Response Plan and Continuity of Operations Plans, following a ransomware attack. These plans all fall in the response phase, they are all reactive.

Prevention and Mitigation are major pillars of Emergency Management. If the hazard can be eliminated, there is a higher chance of reducing or eradicating the potential impact.

Ransomware attacks have very real-world kinetic effects. In 2016, hackers used Samas, or "samsam," which is a virus-like software, to scan the Internet for vulnerable JBoss servers,

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

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.

2. The specific sanction for ransomware possession also gives prosecutors a wider range of options in cases when the evidence for extortion charges may be difficult to prove. HB 215 shifts the focus of prosecution to mere possession of ransomware malware. As such, the search for evidence will be localized to the computer system of the suspect and there is no longer a need to trace a ransomware attack back to a source nor prove the resulting harm of the attack.

3. The *ex ante* enforcement that HB 215 establishes, ensures a concrete deterrent for potential attackers, who will now have to be wary of prosecution from the moment they come into possession of ransomware.

4. Having a standalone specific criminal sanction for ransomware, separate from extortion, considerably increases the possible penalties for ransomware attacks.

HB 215 follows other states that have passed legislation which explicitly addresses ransomware

HB 215 follows legislation that has passed in other states which explicitly address ransomware. California, Connecticut, Michigan, Texas and Wyoming have all passed laws on ransomware.[5] In 2018, Michigan made possession of ransomware software with intent to use it illegal.[6] The threat and cost of ransomware are giving rise to a trend of states passing legislation on this issue.

For all of the foregoing reasons, I strongly support HB 215.

[5] See National Conference of State Legislatures , available at: http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

[6] Michigan House Bill 5258 http://www.legislature.mi.gov/(S(j1qvlqp1cd3e4basocvc3x25))/mileg.aspx?page=GetObject&objectname=2017-HB-5258