Testimony in Support of SB 0030 (2020)

Criminal Law – Crimes Involving Computers – Ransomware

Judicial Proceedings Committee, January 14, 2020

Sponsor: Senator Susan C. Lee

Testimony by: Markus Rauschecker, JD, Cybersecurity Program Director, University of Maryland Center for Health & Homeland Security (CHHS) and Adjunct Faculty at University of Maryland Francis King Carey School of Law

I offer this testimony in support of SB 0030 in my personal capacity. This testimony was prepared with the helpful assistance of CHHS externs: Oluwatosin Ajayi; Nicky Arenberg Nissin; Benita David-Akoro; and Shravana Sidhu.

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.[1]

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.

SB 0030 establishes necessary and strong deterrents against the use of ransomware

By explicitly outlawing the possession of ransomware with the intent to use it, SB 0030 establishes a strong deterrent against this type of malicious software. SB 0030 makes it very clear to cybercriminals that the mere possession of ransomware with the intent to use it is a crime.

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

Moreover, SB 0030 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

SB0030 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, SB 0030 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.

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. SB 0030 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 SB 0030 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.

SB 0030 follows other states that have passed legislation which explicitly addresses ransomware

SB 0030 follows legislation that has passed in other states which explicitly address ransomware. California, Connecticut, Michigan, Texas and Wyoming have all passed laws on ransomware.[2] In 2018, Michigan made possession of ransomware software with intent to use it illegal.[3] 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 SB 0030.

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

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