Statement of

Kyung-shick Choi, Ph.D.
Cybercriminologist & Cybercrime Analyst

Before

Joint Committee on Consumer Protection and Professional Licensure State House

Hearing on

"An Act Addressing Cybercrime Through Enhanced Criminal Penalties, Civil Remedies, and Transparency"

June 20, 2017

Introduction

Thank you for the opportunity to testify on the current state of efforts by the Massachusetts government to minimize the issues of cybercrime facing the Commonwealth.

My name is Kyung-shick Choi. I am both a Professor in the Criminal Justice Department at Bridgewater State University, and the Cybercrime Investigation and Cybersecurity (CIC) Program Coordinator at Boston University. I have been studying and teaching cybercrime and cybersecurity related courses for over 10 years.

As the cybercrime program coordinator at Boston University, I oversee the graduate certificate program in *Cybercrime Investigation and Cybersecurity (CIC)* and teach an average of 80 to 100 law enforcement officers each semester. Since 2009, I have been facilitating the *UN Virtual Forum against Cybercrime* as both an instructor and a cybercrime expert. I have also provided cybercrime training to law enforcement officers and international communities through global cybercrime conferences and local community events as an invited speaker.

My research focuses on the intersection of human behavior and technology—and how criminal justice can respond effectively to the challenges of cybercrime.

Upon thorough review, I am here to support the proposed bill HD3618 as a cybercrime expert.

I see the proposed bill as being divided into three main goals and purposes.

SECTION 2

First, the bill clarifies the liability of damages from security breaches, reflecting the various circumstances in **Section 2**. In fact, cybercrime related legal statues are still ambiguous. This is

because the criminal justice system has not yet caught up with the rapidly evolving dynamics of current technology and its related issues. Given the importance of citizen and consumer trust in both public and private institutions, data breaches can be catastrophic for businesses and citizens' safety. Therefore, specific guidelines for liability and civil remedies should be provided by the state. In this regard, I believe that the proposed bill meets these needs for the state of Massachusetts.

SECTION 4, 5, 6, 7, 8, 9, and 10

Secondly, with the assistance of section 4 (which clarifies specific cybersecurity and cybercrime related terminologies), the bill emphasizes the sanctions and regulations against cybercrimes in **sections 5 (Regulations), 6 (Security Freeze), 7 (Criminal penalties for defraud-related matters), 8 (Extension of dates in criminal penalties), 9 (criminal penalties on cyber breaches), and 10 (duration of imprisonment based on DDOS and potentially Ransomware attack)**. As a society, our reactions and responses to cybercrime incidents are less intense when compared to conventional street crimes. Mass media tend to publicize cybercrimes less frequently unless the particular instances engender substantial harm and pose significant risks to society. Thus, cybercrimes tend to embody low profiles within society and social thought – that is, the public may not label cybercrime activities as "crime". This is further illustrated by the fact that cybercrime cases usually go through civil, and not criminal courts. Although public and private sectors desire investigations into cyber-attacks, they usually avoid contact with the police department. One possible reason could be that the public does not realize the seriousness of cybercrime issues. In this regard, the proposed bill clearly attempts to change the public's perception of cybercrime by increasing the level of sanction placed on data breaches and unauthorized access, as well as adding a new criminal offense for denial of service-type attacks. This bill is a much needed initial step in reframing the traditional criminal justice system, as it takes the lead on changing the paradigm, which is crucial for minimizing potential cyber threats.

SECTION 3

Thirdly, the bill aims to build a special commission on cybersecurity to assess the various cybersecurity threats and prevent potential cyberattacks with risk-management strategies and response plans. This is highlighted in **Section 3**. I would like to discuss this third purpose in more detail because I personally believe that this is the most important objective of the bill.

If you are a victim of a violent crime, you will immediately call 911. Let's say you are a victim of ID theft: Who would you call? Would you know where to go for assistance? Research has shown that most of our citizens do not contact government agencies. That is, while identity theft has been on the rise in recent years — in 2016 alone, around 15.4 million individuals fell victim to this cybercrime – people are still puzzled as to who they *should* and who they *could* report these incidents to. This reflects the findings that, although many citizens become victims of ID theft, most citizens do not rely on law enforcement or government agencies because the majority of citizens believe that there is nothing that the government can do to assist them in their victimization. I wish that I were engaging in hyperbole; I wish that my words were exaggerations. Sadly, this is the current reality of the situation.[1]

[1] Kyung-shick Choi, H. Lim, and S. Back, "Macro-Level Social Opportunity Factors and Cyber Threats: Cybercrime and Its Challenges," Social Forces, For Review 2017.

In one of my recent studies, I found that ransomware attacks occurred in 6 different states (Alabama, Illinois, Massachusetts, Maine, New Hampshire, and Tennessee), whereby 11 local police departments and 2 sheriff departments were affected.[2] Eighty-five percent (85%) (11 out of 13 cases) of police departments paid the ransom demanded via the Bitcoin payment system. Bitcoin is a revolutionary technology that allows for a new way to send payments over the Internet. It is the first ever digital currency in the world. With Bitcoin, you can send any amount of money to anyone and anywhere in the world. The unique thing about Bitcoin is that the transaction is almost impossible to track, and the process is as easy as sending an email. All the ransomware attacks examined in the study came from spear-phishing emails containing hyperlinks and attachments, which infected data encryption.[3] Unfortunately, we had 3 cases in Massachusetts, and all three police departments paid ransoms to these cybercriminals. Ransomware attacks are continually on the rise, and will keep gaining momentum if ransoms are paid.

Another example of such an attack is the recently publicized WannaCry crisis. The WannaCry crisis is the latest ransomware that infected Windows computer systems globally affecting hospitals, universities, government agencies, businesses, and individuals. Starting May 12, 2017, WannaCry infected over 300,000 computers in 150 countries within 72 hours.[4] The identities of the attackers are still unknown.

Furthermore, Ransom Denial of Service attacks (RDos) are also rising in popularity. These attacks, combining the concept of ransomware attacks and distributed denial-of-service attacks (DDos), threaten to conduct a DDos attack against an organization if they do not pay a ransom. This type of cyberattack denies access to the network and can cost organizations millions of dollars in some cases. Cybercriminals' techniques for targeting potential victims have been constantly evolving. According to the Kaspersky Lab, we see over 323,000 new pieces of malware every day and approximately, 37,000 websites are hacked daily.[5]

We are currently faced with a very difficult situation. How are institutions and communities going to react to ransomware, DDOS attacks, and other cyber-attacks in the future? Do we have a structured government policy and/or organizational procedures in place to safeguard victims from such attacks? The "special commission" (listed in line 21) may be the perfect strategy articulator to prepare structured policy and procedures of cyber-crisis scenarios in both public and private sectors.

This bill emphasizes the role of the special commission in promoting the prevention of cybercrime through a refined collaboration among local, state, and federal law enforcement across national and international jurisdictions. This is a crucial element for protecting citizens

---

[2] Kyung-shick Choi, T.M. Scott, and Daniel P. LeClair, "Ransomware against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory," International Journal of Forensic Science & Pathology 4, no. 7 (July 23, 2016).

[3] Choi, Scott, and LeClair, "Ransomware against."

[4] 1. Bill Chappell to NPR newsgroup, "WannaCry Ransomware: What We Know Monday," May 15, 2017, accessed June 7, 2017, http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

[5] Sarah Kitsos, "Kaspersky Lab Number of the Year 2016: 323,000 Pieces of Malware Detected Daily," news release, December 6, 2016, accessed June 12, 2017, http://www.kasperskyforbusiness.com/about-us/press-center/press-releases/2016/Kaspersky_Lab_Number_of_the_Year_2016_323000_Pieces_of_Malware_Detected_Daily.

from cybercrime threats. Cybersecurity is not just a "new thing"; it is the future of law enforcement. However, we have a very small number of units that are capable of operating cyber investigation. Almost every crime has a technological aspect (i.e., an email, a Facebook post, data from smart phone, google maps information, etc.). Additionally, on the darknet, the online drug market has been growing and expanding their drug-trafficking and distributions. Therefore, constant police training and collaboration with all levels of law enforcement in cybercrime investigation is key to combat cybercrime issues.[6]

Constant assessment of cybersecurity threats, detailed preventive risk-management planning, and cybersecurity breach response plans with response notification requirements must be accompanied and coordinated by the state. This is another essential need that the bill clearly identifies.

My recent study on cyber-terrorism indicates that cyberterrorism facilitated by social networking services (such as Facebook, Twitter, and YouTube) or encryption technology can indirectly lead to physical terrorism incidents as seen in many European countries. I strongly believe that this bill can serve to minimize the aforementioned potential risks. Furthermore, I also believe that this bill can strengthen law enforcement agencies' capability of handling cybercrime issues, thereby bridging the trust between government agencies and its citizens.[7]

The greatest way of minimizing cybercrime threats within the state and at the local level would be through active community engagement in raising awareness of potential cybercrime activity on the Internet. Local and state law enforcement should inform their citizens to be alert of suspicious online activity and encourage them to report such behavior to a dedicated unit. Ideally, government and state agencies should train a community network on how to recognize potential cybercriminals and to report suspicious activities to law enforcement agencies.[8]

Educating the general public can be an effective strategy in minimizing the potential risks of cybercrime. Another aspect of public education that is of paramount importance is providing general knowledge of cybersecurity to the masses. For instance, informing the public on the importance of updating security patches, regularly doing data back-ups, and securing home wireless networks can potentially minimize the number of people affected by cybercrime victimization.[9]

This bill broadly emphasizes the need for effective programs and practices as a recommendation. I hope to see this bill in motion and actively facilitating the innovative and effective programs that I addressed earlier. It is my utmost hope that the bill conveys the positive outcomes of minimizing potential cyber threats in both our society and the global community. This concludes my testimony to support this bill. Thank you.

---

[6] Kyung-shick Choi, Cybercriminology and Digital Investigation (El Paso, TX: LFB Scholarly Publishing, 2015).
[7] Kyung-shick Choi, K. Lee, and R. Cardigan, "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS," European Journal of Criminology, Under Review 2017.
[8] Choi, Cybercriminology and Digital.
[9] Choi, Cybercriminology and Digital.

Bibliography

Chappell, Bill. Bill Chappell to NPR newsgroup, "WannaCry Ransomware: What We Know Monday," May 15, 2017. Accessed June 7, 2017. http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

Choi, Kyung-shick. *Cybercriminology and Digital Investigation*. El Paso, TX: LFB Scholarly Publishing, 2015.

Choi, Kyung-shick, Kevin J. Earl, Arang Park, and Jo-Ann Della Giustina. "Use of Synthetic Cathinones: Legal Issues and Availability of Darknet." *VFAC (Virtual Forum Against Cybercrime) Review* Sept/Oct, no. 7 (2014): 19-32.

Choi, Kyung-shick, C. Lee, and R. Cardigan. "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS." *European Journal of Criminology*, Under Review 2017.

Choi, Kyung-shick, H. Lim, and S. Back. "Macro-Level Social Opportunity Factors and Cyber Threats: Cybercrime and Its Challenges." *Social Forces,* For Review 2017.

Choi, Kyung-shick, T.M. Scott, and Daniel P. LeClair. "Ransomware against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory." *International Journal of Forensic Science & Pathology* 4, no. 7 (July 23, 2016): 253-258.

Kitsos, Sarah. "Kaspersky Lab Number of the Year 2016: 323,000 Pieces of Malware Detected Daily." News release. December 6, 2016. Accessed June 12, 2017. http://www.kasperskyforbusiness.com/about-us/press-center/press-releases/2016/Kaspersky_Lab_Number_of_the_Year_2016_323000_Pieces_of_Malware_Detected_Daily.