TO: Mr. Paul Sagan, Chairman of the Massachusetts Board of Elementary and Secondary Education

FROM: Xiaoyu Shi, Tufts University

SUBJECT: Improving Cyber Security Infrastructure in Massachusetts High Schools

DATE: April 21, 2017

PURPOSE

This policy memorandum proposes policy guidelines to address cyber security enhancement in high school infrastructure. Cyber security infrastructure in schools includes physical construction of network hardware, security in school technological systems, and the storage, use, and delivery of data. Poor cyber security infrastructure could result in privacy breaches, interference in school operations, or other serious consequences. As an effort to prevent potential cyber security threats targeting high schools, this memorandum advises the Massachusetts Department of Elementary and Secondary Education (ESE) to issue cyber security assessments, establish state regulations, and organize security trainings in high schools.

BACKGROUND

First, high schools in Massachusetts have established standardized curriculum of technology and engineering in the recent years; corresponding technological tools and systems have widely been set up according to the *2016 Massachusetts Science and Technology/Engineering Curriculum Framework*.[1] However, the *Framework* is deficient in addressing security standards regarding technologies widely used in high schools, such as Local Area Networks (LAN), wireless connections, and student accounts and registration.

Second, high schools in Massachusetts are expected to pertain a student record system[2], and are supposed to collect data upon request of Data Collection Programs of ESE.[3] However, ESE fails to provide a guideline for data storage and database security, and allows much liberty in data storage, delivery, and duration of obtainment in high schools.

Third, with diversification of cyber security threats and the proliferation of available cyber exploitation tools, malicious cyber security attacks in high schools have increased in the recent years. For example, in Feburary 2017, phishing scams have victimized more than 20 school districts in over ten states, resulting in loss of private information.[4] Additionally, the hacks of New Dorp High School[5], Ormsby School[6], and Iroquois Central School District[7] in 2016 suggest that high schools have become "an easy target" for cyber security exploitations according to experts, and sometimes attract arranged crimes for social security numbers and personal information.[8]

POLICY OPERATIONS

1. ESE. *2016 Massachusetts Science and Technology/Engineering Curriculum Framework*. Apr. 2016
2. ESE. Education Laws and Regulations: Student Records. Feb. 2005.
3. ESE. Information Services: Data Collection. Jan. 2017.
4. Herold, B. *Phishing Scam Targets School Employees' Information*. <http://blogs.edweek.org/edweek/DigitalEducation/2017/02/phishing_scam_targets_schools.html>. Feb. 2017.
5. Donnelly, F. *Teen admits to hacking New Dorp High School student records*. <http://www.silive.com/eastshore/index.ssf/2016/01/teen_admits_to_hacking_new_dor.html>. Jan. 2016.

6. 7. 8. Elsufon, R. *Expert: Schools at risk for hacking attacks*. <http://www.wkbw.com/news/expert-school-districts-at-risk-for-hacking-attacks>. Apr. 6, 2016.

1. Conduct Assessment on High School Cyber Security Infrastructure

In November 2014, the U.S Department of Education has issued a handbook *Future Ready Schools: Building Technology Infrastructure for Learning* in support of the U.S. Department of Education's National Educational Technology Plan (NETP).[9] *Future Ready Schools* provided security recommendations in high school infrastructures, such as the necessities of reliable LAN connections in schools, network traffic and content assessment, and database persistence. ESE could conduct cyber security assessments to help schools and districts reflect on current installation and application of technologies. The assessment should include: 1) systematically identify existing technological infrastructures and practices; 2) discuss what is currently useful and effective in cyber threat prevention; 3) formulate actions that are necessary to address identified gaps; and 4) establish a coordinated district-wide plan for cyber threat information sharing.

2. Establish State-Wide Regulations for Cyber Security Infrastructure in High Schools

ESE could further expand the recommendations and instructions given by *Future Ready Schools* into state-wide regulations on cyber security infrastructure. The regulations should cover both topics regarding technological systems construction and data handling. Regulations issued by the ESE could prohibit the adoption of easily-exploitable practices such as lack of hardware and services such as firewalls and content filtering, use of unreliable or outdated network equipment, unsafe information sharing systems between schools and districts, and the use of insecure databases. The regulations could also include requirements for regular updates and assessments of cyber security infrastructure.

3. Prevent Social Engineering and Other Vulnerabilities by Cyber Security Training

The Office of Digital Learning (ODL) was founded under ESE to sustain education curriculums supported by technology.[10] In addition to incorporate technologies into schools, ODL should educate students and educators defensive measures against cyber exploitations that come with new technologies. Education campaigns organized by the ODL could include identification of social engineering exploitations such as phishing and baiting, prevention of poorly-constructed networks such as those with overly-permissive whitelists[11], prevention of weak password requirements[12], and education of cyber ethics and regulations that prevents active hacking attempts from students and educators.

RECOMMENDATIONS

The policy operations could be divided into two major aspects. Recommendations 1 and 2 addresses the problem with technical solutions and system enhancements, while recommendation 3 notifies the lack of security training and the backward mentality facing cyber threats. According to my experience in John D. O'Bryant School of Mathematics and Science, Boston, MA, cyber security assurance in high schools needs efforts from both technical and human aspects. Although the incorporation of technology has been on the agenda of ESE for years, limited achievements have been made to address cyber security according to default passwords on computer login, simple Wifi passwords, and the lack of awareness in counter-

[9] Office of Educational Technology, U.S. Department of Education. *Future Ready Schools: Building Technology Infrastructure for Learning*. Page 6-8. Nov. 2014.
[10] ECE. Office of Digital Learning: Home. < http://www.doe.mass.edu/odl/>. Mar. 2017.
[11] CWE-942: Overly Permissive Cross-domain Whitelist.
[12] CWE-521: Weak Password Requirements.

cyber exploitation practices. I recommend that the ESE start with simple assessments (recommendation 1) and education (recommendation 3), which addresses both technical and human factors, then gradually proceed to enhancing high school cyber security infrastructure via legislations (recommendation 2).