NCSL
NATIONAL CONFERENCE OF STATE LEGISLATURES

NCSL Executive Task Force on Cybersecurity
April-May 2020

Task Force Highlights

Regrettably, we must cancel our July meeting in Cambridge, Mass., but we are planning a series of virtual meetings to cover the topics we were planning to examine in person.

Thanks to everyone who attended our first virtual meeting in April. Our next virtual meeting will be held **May 28 at 3 p.m. Eastern.** Please join us to hear about ransomware and cybersecurity training legislation enacted in Texas, sponsored by Task Force member Representative Giovanni Capriglione, and learn how Atlanta handled its ransomware attack in 2018 from our sponsor Forescouts' Senior Systems Engineer Jonathan Jesse, who helped the city recover.

On **June 25 at 10:00 a.m. Pacific and June 26 at 9:30 a.m. Eastern,** task force members will be able to participate in a **virtual incident response challenge**, normally held at the IBM X-Force Command Center in Cambridge, Mass. These briefings from our task force sponsor will simulate how a breach unfolds in real time and showcase the attack vectors that health care, life sciences, education and government organizations experience every day. Attendees will gain a greater understanding of security best practices and tactics, the importance of implementing a security strategy and the leadership skills required to deal with a major security issue.

Federal Cyber Snippets

- The Cybersecurity and Infrastructure Security Agency (CISA) published a CISA Insights document on disinformation. This publication provides tips on how to identify disinformation on the internet and how to prevent amplifying disinformation campaigns by verifying information with trusted sources such as FEMA.gov or coronavirus.gov before forwarding links. CISA is also publishing information on cyberthreats related to COVID-19 on a regular basis, most recently addressing threats to the health care and pharmaceutical industries. CISA has also released two supply chain risk management (SCRM) products to help businesses and organizations enhance the security and resiliency of their supply chain networks.
- The U.S. House of Representatives recently introduced the Health and Economic Recovery Omnibus Emergency Solutions (HEROES) Act. The bill appropriates $3.6 billion for contingency planning, preparation and resilience of elections for federal office. This funding includes making

elections cyber secure. The bill also provides that funding under the previously enacted CARES Act can bypass the state legislature and go directly to the chief election official of each state.

- ★ The Senate Homeland Security Committee held its first virtual hearing on the Cyberspace Solarium Commission's report. All witnesses were members of the commission. Chairman Ron Johnson (R-Wis.) stressed the need for better information sharing on the threat landscape and his support for the commission's recommendation for a national cybersecurity director. Ranking Member Gary Peters (D-Mich.) endorsed the commission's recommendations. Commission members emphasized the need for a layered cybersecurity approach nationwide.
- ★ ICE and the Homeland Security Child Exploitation Investigations Unit launched Project iGuardian for school systems and youth organizations. The goal of iGuardian is to provide parents, teachers and students information about the dangers of online environments, how to stay safe online, and how to report abuse and suspicious activity, especially while kids are using online learning platforms during COVID-19.

State Action

Cybersecurity Legislation 2020

State legislative sessions began in typical fashion in early 2020. Within a few weeks, however, the coronavirus (COVID-19) spread, and legislatures began postponing or cutting sessions short, closing capitols, or meeting virtually and voting remotely. Legislation since has largely focused on coronavirus issues. So, while the number of cybersecurity bills introduced this year is somewhat higher than the number introduced last year, enactments are down significantly.

Bills enacted so far in 2020 include the following:

State/Bill	Title
Georgia HB 792	Appropriations for State Government Operation
Indiana HB 1372	Insurance Data Security
Indiana SB 179	Election Cybersecurity
Indiana SB 334	Election Security
New Mexico HB 2	General Appropriation Act
South Dakota HB 1044	Cyber Incubator and Entrepreneurial Center Development
Utah HB 41	Water Policies (cybersecurity)
Virginia HB 852	Information Technologies Agency (training requirements)
Virginia HB 1082	Emergency Services and Disaster Law
Virginia HB 1334	Insurance Data Security
Virginia SB 378	Computer Trespass Penalty
Virginia SB 1003	Computer Crimes
Washington HB 1251	Election System Data Security Breaches
West Virginia SB 261	Computer Ransomware Penalty

Insurance Data Security

The National Association of Insurance Commissioners (NAIC) in October 2017 adopted the Insurance Data Security Model Law. The purpose of the model law is to "establish standards for data security and standards for the investigation and notification to the Commissioner of a Cybersecurity Event applicable to Licensees." Indiana and Virginia, by enacting legislation this year, bring the number of states adopting the model law to 10: Alabama, Connecticut, Delaware, Indiana, Michigan, Mississippi, New Hampshire, Ohio, South Carolina and Virginia.

International

- ★ The University of Portsmouth in the U.K. published a report on the victims of cybercrime to shed light on law enforcement response, victims' support, and prevention strategies. This report revealed that police response was low among those interviewed, and that the types of hacking varied from ransomware to malware to phishing.