Hartford Courant May 4, 2018

Stronger Cyber Defenses Urged

Malloy Plan Calls For Better Security

By STEPHEN SINGER ssinger@courant.com

A state cybersecurity plan issued Thursday calls for more extensive security in state agencies, the General Assembly and judicial branch, establishing municipal cyber defenses and other changes to protect confidential data and digital information.

Gov. Dannel P. Malloy said his administration's plan offers ways to prepare for, respond to and recover from the consequences of cyber compromise.

"The plan itself does not make us safe; it gives us a way to work toward safety," he said.

A ransomware attack knocked the state court system's computers offline in March, affecting 114 servers. A similar bug hit more than 100 computers in 12 state agencies in February.

The 41-page plan calls on the General Assembly to approve a resolution insisting that Connecticut is vulnerable to "cyber compromise" and that action to strengthen cybersecurity is a state priority. The resolution should call on every agency to create its own plan consistent with the state's cybersecurity strategy and the state plan.

The goal of Connecticut's cybersecurity response and recovery plan is to anticipate the dimensions and challenges a cyberattack or cyber failure would have on Connecticut's infrastructure, the plan said.

State agencies also should have a recovery plan, including continuity of operations planning based on "worst-assumption scenarios" and rehearse recovery steps in annual exercises, according to the plan.

The report said the business community must demonstrate it understands its role and is prepared to protect individuals' data. A key goal of Connecticut's plan is for businesses to recognize threats and to put in place "serious, effective programs that distinguish Connecticut businesses as active partners in the state's cybersecurity efforts."

The plan said the business community knows best how to create an "effective cybersecurity business climate," but added that state law is also an option to compel businesses to protect computer systems.

"Where necessary goals are not achievable by voluntary action, inevitably the political process will look to legislation and regulation, as has New York state with its promulgation of cybersecurity requirements for financial service companies," the plan said. "For many businesses, fear of and opposition to legislation and regulation dominate their thinking about cybersecurity, and they approach the subject with some suspicion and resentment. Yet cybersecurity has become a compelling public issue."

Joe Brennan, president of the Connecticut Business and Industry Association, said the state's largest business group met with state officials as the report was being drafted and worked with member businesses about how to strengthen cybersecurity protections.

Cybersecurity requirements vary among different businesses, such as hospitals that hold confidential health records, defense contractors with data that touch on national security, insurance companies with

homeowners' records and utilities that are responsible for electricity and gas deliveries. As a result, businesses will resist a "one-size-fits-all" government plan, Brennan said.

"We're trying to avoid a heavy regulatory scheme," he said.

A July 2017 state report recommended improved knowledge to identify and prevent cyber intrusions, skills to handle cybersecurity tasks, better preparation, specific response plans, recovery operations to identify damage, analysis of the causes, information-sharing and verifying if efforts to reduce cybersecurity risks are working.