Scott to form cybersecurity panel

Baltimore Council president's move follows crippling computer hack

Rapid Response Crisis Team

Scott

By Doug Donovan The Baltimore Sun

Baltimore City Council President Brandon Scott announced Thursday that he is convening a special committee focused on cybersecurity and emergency preparedness as City Hall struggles to recover from a hack that has crippled the government's email and other computer systems.

The ransomware attack last week on the city's computer network has caused widespread problems across agencies, including shutting down systems essential for completing home sales in Baltimore.

Emergency Management Model

"This cyberattack against Baltimore city government is a crisis of the utmost urgency," Scott said.

The new council president said the committee will invite testimony from experts to help review the response to the attack by Democratic Mayor Bernard C. "Jack" Young's administration and examine the city's cybersecurity policies and emergency plans.

Budget documents show that the city's information technology office has blamed funding cuts for limiting some of its efforts to bolster cybersecurity training.

"I've been telling administrations for years that they need to spend more on cybersecurity," Scott said, referring to previous mayors' strategies, not Young's new administration.

At a budget hearing last year, Scott reminded information technology officials that Baltimore's 911 dispatch system had been recently been hacked and shut down for a weekend. "I don't think the city spends enough money to make ourselves safe from cyberattacks," he said at the time. Gayle Guilford, an information technology official, responded, saying, "We have made some progress, but not enough. We continue to beg and plead. I need some help, and I need some money."

The city fell victim May 7 to new hackers demanding payment to unlock encrypted files in city computers.

Young has said the city will not pay a ransom to the destructive virus, called RobbinHood, which city officials have described as "very aggressive."

"The Baltimore City Council and I stand ready to work with the administration and our federal partners, including the FBI and, if appropriate, the Department of Homeland Security, to resolve the crisis, support the criminal investigation and take active steps to prevent this from happening again," Scott said.

Scott said Democratic Councilmen Eric Costello and Isaac "Yitzy" Schleifer will serve as co-chairmen of the committee.

Scott said he is thankful that critical services such as public safety, water and public works were able to operate without interruption despite the ransomware attack.

"The bad news is that we don't know when this threat will end or who is perpetrating this attack on our city and the services that we provide," the Democrat said.

Costello previously worked for nearly nine years as a senior information technology auditor at the U.S. Government Accountability Office.

"I'm bringing professional expertise to this," Costello said.

The councilman said the committee's scope is being formulated, but he has already connected with cybersecurity experts who could participate in hearings. The committee will discuss how the current incident transpired, examine the city's response, review existing policies and explore "any changes that need to happen," he added.

Costello said the council has to determine how to work within the state's open meetings law when discussing sensitive matters.

"There will be things that can't be discussed publicly," he said. "When we discuss what our vulnerabilities are, that's not information we want hackers to have access to."

Lester Davis, a spokesman for Young, said the committee is expected to begin its work in the fall. The timing will allow the administration to restore its computer system and install stronger mechanisms to guard against attacks.

"There are going to be lessons to be learned from this," Davis said.

Young has instructed agencies to document those lessons while they're working to restore the computer systems to minimize the chance of future attacks crippling City Hall computers.

The disruption to the computer network has caused widespread problems. City employees do not have access to email, and several agencies are using workarounds to continue offering services that rely on computers. The hack has affected the city's ability to pay its bills and accept payments — including property taxes.

Officials have stressed that emergency services, including 911 and 311, are not affected, but they acknowledged that the Baltimore Police Department email system is not working. Police spokesman Matt Jablow said the department cut off access to CitiWatch cameras in Baltimore's nine police districts as a precaution because the stations plug into video feeds through the city's computer network. He said headquarters can provide information from CitiWatch to the districts.

On Wednesday, the mayor said city technology employees are working with the FBI, Microsoft and other vendors to help restore computer services. But an ongoing criminal investigation has prevented city officials from disclosing much information for fear of sharing details that could reveal vulnerabilities to hackers.

Officials would not disclose which companies are working with them to restore systems. And the city's information technology officer, Frank Johnson, has declined to say whether the city had an emergency plan in place for such an attack.

A review of city budgets shows that certain elements of cybersecurity strategy has lagged as funding has declined.

An "Information Security Office" was first funded in the city's fiscal 2016 budget "to develop cybersecurity technology, policies and trainings and to respond to information security incidents." One of its stated goals in the spending plan was to provided 32 "cybersecurity awareness trainings."

The budget for that first year was $532,567 to pay for "one city and two contract positions" in the office.

The spending plan for the following year increased to about $543,000, but the city only spent $189,027, budget record showed. And in fiscal 2018, information security spent $456,965, 33% below its nearly $685,000 budget.

In addition, every subsequent budget since 2016 no longer mentions "cybersecurity awareness trainings" or whether the agency achieved its goal of 32 sessions.

Instead, each budget from fiscal year 2017 through the current spending plan repeats the goal of working to "improve the city's overall cybersecurity posture."

Part of that effort has been a goal of "modernizing" applications on the city's computer mainframes. The target was to modernize 38 applications in fiscal year 2016. But only one was modernized — the city's water billing application, according to budget documents.

"No applications were modernized in fiscal 2017 due to the lapse of capital funding," budget documents state. "In fiscal 2018, [the agency] does not expect mainframe modernization to occur due to lack of funding, and consequently set lower performance targets."

But in fiscal year 2018, the city did recommended a capital budget of $500,000 to implement a citywide cyber security policy and auditing tools to protect against cyberattacks.

In November 2017, Baltimore's spending board approved a $500,000 transfer to the information technology agency to "allow for the implementation of an added tier of cybersecurity and malware protection that would protect against zero-day exploits and advanced persistent threats" and provide analysis of malware attacks.

Baltimore Sun reporter Jessica Anderson contributed to this article.

ddonovan@baltsun.com

twitter.com/dougdonovan