A Times editorial

Federal aid needed for cybersecurity

The newest threat facing cities and states is not climate change or illegal immigration but cyberattacks that have crippled dozens of municipalities — large and small alike — and costs taxpayers millions in ransom and damages. This problem will only worsen, as more routine government functions go online and as cash-strapped cities and states struggle to afford adding cybersecurity to protect this vital infrastructure. The federal government should make security grants and technical assistance more available before more vulnerable communities are held hostage.

A string of reports this summer reveals the extent of the growing cybersecurity crisis. More than 40 municipalities have been victims of cyberattacks this year, from large cities such as Baltimore and Albany to small Florida towns like Lake City and Riviera Beach. The two Florida cities paid a combined $1 million plus after ransomware attacks this year. Hackers are using sophisticated tools and organized means to attack public computer systems across the country, often targeting smaller towns that lack the budgets to proactively defend their computer systems. The ransom payments are expensive and questionable public policy, but government officials contend they were the least expensive alternative.

Imagine the normal function of everyday life going dark — computers in police cars and libraries shutting down, billings and phone systems disabled, emails disappearing into the ether. Ransomware doesn't destroy data or equipment; it locks out users until they meet a hacker's demand — typically a large amount of money.

Some cities have bought cyberinsurance, which may protect a government agency but raises the risk of encouraging a run on the system. And buying insurance underscores the larger problem; many cities, especially smaller ones, lack the money, staffing and technical expertise to adequately insulate their computer systems. That's one reason why communities that balk at paying five-figure ransoms can end up facing multimillion dollar costs for lost revenue and system upgrades as they recover from an attack.

A study last year by financial services giant Deloitte and the National Association of State Chief Information Officers found that almost half the states do not have a line item in their budgets for cybersecurity, and that in most, cybersecurity accounts for only 1 to 2 percent of the overall information technology budget. By comparison, many civilian agencies in the federal government spend 6 percent or more of their IT budgets on cybersecurity. That figure jumps to an average of 28 percent for the private sector.

The Departments of Justice and Homeland Security provide a range of assistance to states and local communities, from security grants and technical assistance to incident response. But with billions in infrastructure at stake, the federal government needs to play a larger role in addressing these nationwide threats. States and cities need more resources to prepare for and recover from cyberattacks. They also need greater federal assistance in hardening their technologies and detecting potential threats in real time. The costs won't be cheap. But they pale in comparison to the orderly delivery of services and to public confidence in government.