States Confront the Cyber Challenge

Q&A: Ransomware

What is ransomware?

Ransomware is a type of malicious software used by criminal computer hackers to extort money from individuals and organizations. Once loaded onto a victim's computer, the ransomware encrypts hard drives and locks key system functions, preventing victims from accessing important files or using their computer altogether. The hacker then requests payment (usually in an untraceable, digital currency) to an anonymous account, threatening to destroy the victim's files or data if the ransom does not arrive on time. Whereas other cyber attacks seek to steal data or commandeer a computer in secret, the defining feature of ransomware is extortion.

Why do criminal actors use ransomware?

Many varieties of ransomware are available online for free, and they often exploit known security vulnerabilities affecting millions of Internet-connected computers. This means even novice cyber criminals can use ransomware to extort thousands or tens of thousands of dollars in quick fashion. Requesting payment in digital currency allows them to hide from criminal investigators. For these reasons, ransomware has become a popular tool in the criminal underworld.

How is ransomware deployed against the public sector?

Ransomware often targets critical organizational functions:

- In May 2017, a ransomware known as WannaCry rapidly infected hundreds of thousands of computers across the globe. Hundreds of hospitals across the United Kingdom were affected; some were forced to turn away patients at the door.
- A 2016 attack on San Francisco's transportation agency shut down the city's light rail ticketing system for a day, costing the agency the day's fares. The attackers demanded $73,000.
- A 2016 incident at a Los Angeles hospital forced administrators to pay $17,000 to hackers.

How can I defend against ransomware?

Basic cybersecurity hygiene can dramatically reduce the risk of a ransomware attack. Some steps are cheap and effective, such as updating software, blocking suspicious email accounts, and preventing the download of programs that are not pre-approved. Employee training is indispensable, and free training tools are widely available.

Preventive steps such as these will not block all ransomware, nor will they guarantee business continuity in the event of a successful ransomware attack. Thus, the most important step organizations can take to defend against ransomware is to back up data, preferably on separate networks or in the cloud. A school district in New Jersey and a hospital in Kentucky, both victims of ransomware, restored operations without paying because they used backups. In addition, a written business continuity plan stipulating how employees should transition to backups will enable smooth recovery of business operations. However, to be effective, backup measures may require modest budget supplements, as they often entail purchasing new hardware or subscriptions with cloud providers.