GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Snapshot

Ransomware: Federal Coordination and Assistance Challenges

GAO-23-106279 · November 2022

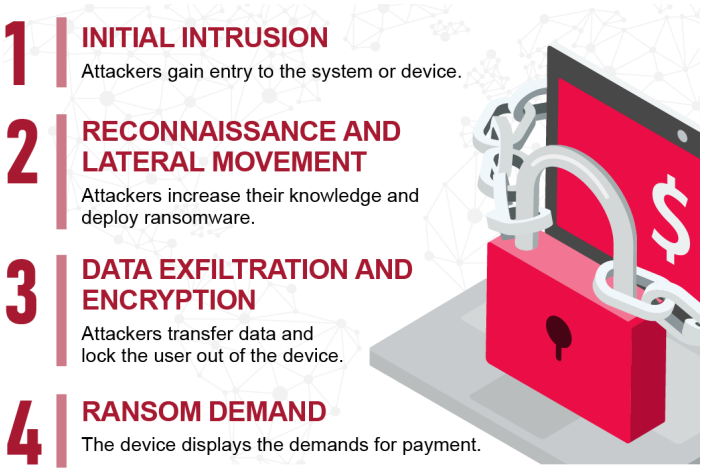
Accessible Version

Ransomware poses threats to federal, state, and local government organizations, including schools. Taking action on three recommendations from our work in this area could help the federal government improve coordination and assistance.

The Big Picture

Ransomware attacks are on the rise at organizations and industries of all sizes. Hospitals, schools, emergency services, and other industries have been the victims of such attacks. Ransomware is a form of malicious software designed to render the underlying data and systems unusable. Ransom payments are then demanded in exchange for restoring access to the locked data and systems.

Four stages of a ransomware attack



Source: GAO analysis based on information from the Cybersecurity and Infrastructure Security Agency, Center for Internet Security, and Federal Bureau of Investigation; image: tomasknopp/stock.adobe.com. | GAO-23-106279

State, local, tribal, and territorial (SLTT) government organizations, including schools, have been particularly targeted by ransomware attacks, which can have devastating impacts on vital government operations and services. According to the Multi-State Information Sharing and Analysis Center—an independent, nonprofit organization—SLTTs experienced approximately 2,800 ransomware incidents from January 2017 through March 2021.

Consequently, federal assistance provided to SLTTs to prevent and respond to ransomware threats is essential to enhancing cybersecurity resiliency and effectiveness.

What GAO's Work Shows

GAO's work identified areas where the federal government could improve the coordination and assistance it provides to others for addressing ransomware attacks.

1. Interagency Coordination

The Cybersecurity and Infrastructure Security Agency (CISA), Secret Service, and FBI are the primary federal agencies that provide direct assistance aimed at preventing and responding to ransomware attacks on SLTTs. This is provided through education and awareness, information sharing and analysis, cybersecurity review and assessment, and incident response.

However, in September 2022, we reported that they lacked processes for more effective federal coordination on ransomware assistance to SLTTs. Specifically, the interagency coordination between the three agencies on ransomware assistance to SLTTs was informal and lacked documented procedures.

- **We recommended** that CISA, Secret Service, and FBI improve interagency coordination on ransomware assistance to SLTTs.

2. Awareness, Outreach, and Communication

In September 2022, we reported that although SLTTs were generally satisfied with the ransomware assistance provided by the federal government, officials from all 13 SLTTs we interviewed identified challenges with awareness, outreach, and communication:

- SLTTs reported difficulties identifying the federal services that were available to them.

- Tribal officials expressed concerns about CISA's focus on conducting outreach at the state level, leaving tribal nations uninformed.
- SLTTs contacting FBI for response assistance cited issues with inconsistent and timely communication.

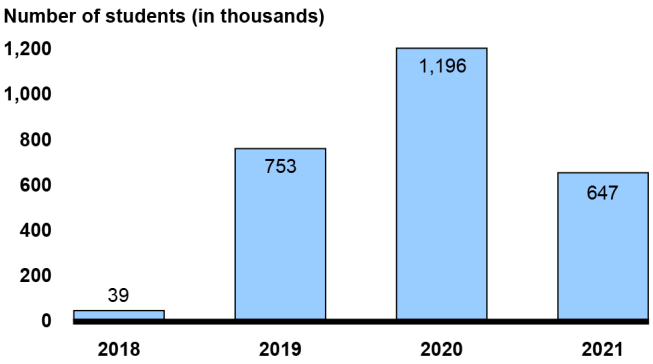
➢ **We recommended** that CISA, Secret Service, and FBI evaluate how to best address concerns raised by SLTTs.

3. Coordination with Schools

Cybersecurity incidents, such as ransomware attacks, at kindergarten through grade 12 (K-12) schools can significantly impact their ability to continue operations and can cause learning and monetary loss.

In October 2022, we reported that state and local officials knowledgeable about K-12 cybersecurity indicated that the loss of learning following an incident ranged from 3 days to 3 weeks, and incident recovery time ranged from 2 to 9 months. In addition, a research organization provided us with an estimate of the number of students being affected by ransomware attacks between 2018 and 2021.

Estimated Number of U.S. Students Affected by Ransomware Attacks on K-12 Schools, 2018-2021



Source: GAO analysis of Comparitech study on K-12 school ransomware attacks. | GAO-23-106279

Federal guidance, such as the 2013 National Infrastructure Protection Plan (National Plan), calls for the development of government coordinating councils to, among other things, enable interagency and intergovernmental coordination to address a specific need for federal assistance, such as cybersecurity at K-12 schools.

However, we found that while the Department of Education and CISA offer cybersecurity resources to K-12 schools, such as online safety guidance, they otherwise have little to no interaction with the K-12 community regarding their cybersecurity.

This is due, in part, to the Department of Education not establishing a government coordinating council, as called for in the National Plan. Such a council can facilitate communication and coordination among federal agencies and with the K-12 community. This, in turn, can enable federal agencies to better address the cybersecurity needs of K-12 schools.

➢ **We recommended** that the Department of Education, in consultation with CISA and other relevant stakeholders, establish an applicable government coordinating council to coordinate cybersecurity efforts between federal agencies and with the K-12 community.

Opportunities

The recently enacted *Consolidated Appropriations Act, 2022* includes requirements for additional federal coordination in addressing ransomware threats. The act requires CISA to lead the establishment of and chair a Joint Ransomware Task Force. Once the task force is established, federal agencies like CISA, Secret Service, and FBI may have a mechanism for coordinating federal ransomware assistance to SLTTs, including schools.

More from GAO's Portfolio

Cybersecurity

Information Technology

Science and Technology

Contact Us

For more information about this Snapshot, contact: Jennifer R. Franks, Director, Information Technology & Cybersecurity, (404) 679-1831

Chuck Young, Managing Director, Public Affairs, (202) 512-4800

A. Nicole Clowers, Managing Director, Congressional Relations, (202) 512-7114

Contributors: Chris Businsky, Kavita Daitnarayan, Donna Epler, Michael Gilmore, Torrey Hardee, Nicole Jarvis (assistant director), Josh Leiling, Scott Pettis, and Umesh Thakkar (analyst-in-charge)

Source (cover photo): kaptn/stock.adobe.com.