GAO
U.S. GOVERNMENT
ACCOUNTABILITY OFFICE
Snapshot

Cyber Resiliency: CrowdStrike Outage Highlights Challenges

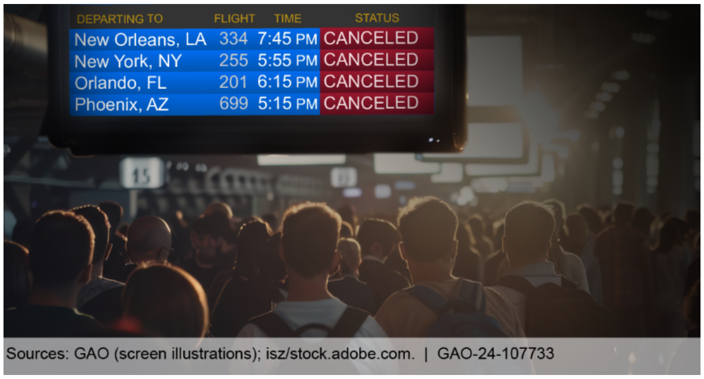
GAO-24-107733 · September 2024

Challenges in supply chain risk management, testing, contingency planning, and cyber information sharing make it more difficult to mitigate cybersecurity risks to IT systems. GAO's work in these areas highlights the need to mitigate them. (Accessible Version)

The Big Picture

In July 2024, a software update from the cybersecurity firm CrowdStrike caused Microsoft Windows operating systems to crash—resulting in potentially one of the largest IT outages in history. The outage disrupted critical infrastructure operations by grounding commercial flights and interrupting critical hospital care, among other impacts.

Depiction of CrowdStrike Outage Effect



DEPARTING TO	FLIGHT	TIME	STATUS
New Orleans, LA	334	7:45 PM	CANCELED
New York, NY	255	5:55 PM	CANCELED
Orlando, FL	201	6:15 PM	CANCELED
Phoenix, AZ	699	5:15 PM	CANCELED

Sources: GAO (screen illustrations); isz/stock.adobe.com. | GAO-24-107733

CrowdStrike's investigation of the incident found that a faulty security update caused widespread system failures, affecting millions of Windows systems. Although the CrowdStrike crash was caused by human error and not a cyberattack, it highlights similar vulnerabilities we saw during the SolarWinds attack in 2019. In that event, instead of attacking systems directly, malicious actors targeted system support software. That software, SolarWinds Orion, was widely used by federal agencies to monitor network activity and manage network devices. This allowed the threat actor to breach several federal networks. Cyber incidents at federal agencies and the nation's critical infrastructure sectors, such as transportation and healthcare, are growing in number, impact, and sophistication. Federal entities, such as the Cybersecurity and Infrastructure Security Agency (CISA), lead efforts to coordinate national cyber policy and critical infrastructure cybersecurity.

What GAO's Work Shows

GAO has long reported on the importance of supply chain risk management, testing, contingency planning, and information sharing to help manage and mitigate cybersecurity vulnerabilities.

- **Supply chain risk management.** Organizations have increased their reliance on complex, interconnected, and global supply chains that can include multiple tiers of outsourcing. The exploitation of IT products and services through the supply chain is an emerging threat.
  - ➢ In 2020, we identified seven practices to manage and protect federal IT against these risks. We made recommendations for improving supply chain risk management practices including detecting counterfeit and compromised technology products prior to their deployment.
- **Testing.** Testing and approving new and modified systems and software (including critical security patches) before their implementation are essential to help ensure systems' hardware and programs operate as intended and that no unauthorized changes are introduced. Our work has found that federal agencies do not always adequately address issues found in testing before deploying new systems or software. This makes it more difficult to protect against cyber risks and system failure.
  - ➢ In 2021, we recommended that the Departments of Defense and Veterans Affairs improve testing processes for their electronic health records systems to verify the systems perform as intended and meet users' needs.
- **Contingency planning.** Contingency planning helps ensure that if operations are interrupted,

organizations are able to detect, mitigate, and recover from a service disruption while preserving access to vital information. However, our work has shown that federal agencies do not always plan for and test their plans for contingencies.

- In 2023, we recommended that the State Department annually test its contingency plans for its systems that have significant impact to the United States' national security interests so the department can better prepare for and respond to incidents when they occur.

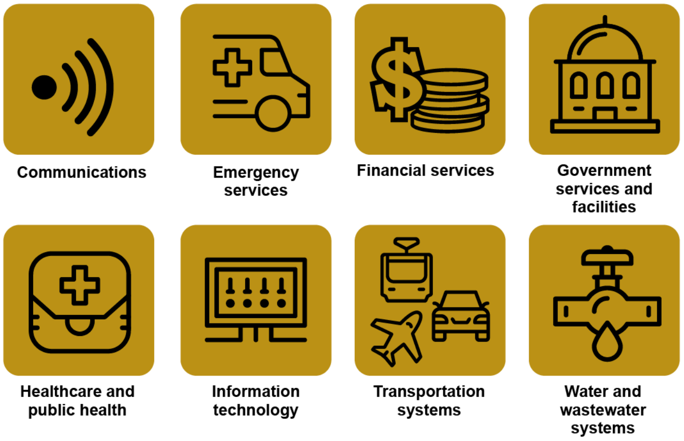
- **Cybersecurity information sharing.** Cyber threats to the nation's critical infrastructure continue to increase and represent a significant national security challenge. As these threats become more complex, it is increasingly important that federal agencies and critical infrastructure owners and operators share cyber threat information. Federal agencies are often challenged in sharing cyber threat information due to lack of voluntary sharing by non-federal entities and actionable information, among others.

  - In 2023, we recommended that the White House and key agencies work to better ensure that information sharing across the government and critical sectors was effective and timely.
  - In 2024, we reported on CISA's efforts to implement legislation on cyber incident reporting for critical infrastructure.

Opportunities

Concerted action among the federal government and its nonfederal partners in critical infrastructure sectors is essential to mitigating the risks posted by cyber-based threats. Therefore, in 2018 we included four major cybersecurity challenges facing the federal government in our High Risk update. The federal government has also taken steps to improve the response to such incidents. But there is still work to be done to improve the way cyber incidents are managed and mitigated.

Examples of Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-24-107733

Our work highlights opportunities to implement needed corrective actions in the federal government's effort to protect against cyberattacks and vulnerabilities. For example, in April 2024, we recommended that key federal agencies implement executive order requirements intended to improve the federal government's response to cybersecurity threats. More broadly, since 2010 we have made 1,624 recommendations in public reports that address the four major cybersecurity challenge areas. As of September 2024, 528 remained unimplemented. Implementation of these recommendations would help to improve the overall cyber resilience of the federal government and critical infrastructure sectors.

The federal government has acted to address the challenges in protecting its systems and those of the critical infrastructure sectors. For example, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022. The act established cyber incident reporting requirements across the 16 critical infrastructure sectors. CISA has efforts underway to finalize a rule that would implement the act's requirements for cyber incident reporting by October 2025. Continued persistence in combating cyber incidents is essential to protecting systems that are vital to the United States.

About GAO:

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. This document is based on GAO audit products.

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.

This work of the United States may include copyrighted material, details at https://www.gao.gov/copyright.

Contact Us:

For more information, contact: Jennifer R. Franks, Director, Center for Enhanced Cybersecurity, IT & Cybersecurity, (404) 679-1831.

Sarah Kaczmarek, Managing Director, Public Affairs, KaczmarekS@gao.gov, (202) 512-4800.

A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400.

Contributors: Anastasia Barron, Chris Businsky, Donna Epler, Nicole Jarvis (Assistant Director), Cassaundra Pham (Analyst-in-Charge), and Kevin Smith.

Source (cover photo): ipopba/stock.adobe.com (background, doctors); magann/stock.adobe.com (airplane).