

< WatchBlog: Following the Federal Dollar

CrowdStrike Chaos Highlights Key Cyber Vulnerabilities with Software Updates

Posted on July 30, 2024



Earlier this month, a software update from the cybersecurity firm CrowdStrike caused Microsoft Windows operating systems to crash—resulting in potentially the largest IT outage in history.

Disruptions were widespread. Around the world, businesses and services were unable to operate as computers crashed, and some critical infrastructure sectors (like transportation, healthcare, and finance) were disrupted. For example, commercial flights were grounded, critical hospital care was interrupted, and financial institutions were unable to service clients.

Here at GAO, we have long [highlighted](#) concerns for Congress about IT vulnerabilities, a lack of security awareness, poor cyber hygiene, and a need for more cyber preventative measures to combat disruptions like the CrowdStrike outage. In our prior work, we have identified risks to the nation's critical infrastructure sectors and in the supply chain of software supporting IT systems.

Today's WatchBlog post looks at this work, including [our June update](#) to the High Risk List.

 Photo illustration showing a busy city road at night with digital icons floating over it in a web.

CrowdStrike crash caused by supply chain vulnerability similar to SolarWinds attack

So far, what we know about the CrowdStrike crash is that it was caused by human error and not a cyberattack or malicious intent. But the crash highlights the same vulnerabilities we saw during the SolarWinds attack in 2019. Instead of attacking systems directly, malicious actors targeted the software used to support them.

SolarWinds attack. Beginning in September 2019, the Russian Foreign Intelligence Service led a campaign of cyberattacks, breaking into the computing networks of SolarWinds—a Texas-based network management software company. The software was widely used by the federal government to monitor activities and manage devices on federal networks.

Hackers injected trojanized (hidden) code into verified SolarWinds software updates. When SolarWinds released the software updates to its customers, the threat actor gained a “backdoor,” or remote access, to customers’ networks and systems. The attack was discovered more than a year later in November 2020.

We provide a timeline of these attacks and the response in our [April 2021 blog post](#).

Protecting the software supply chain. As we saw with CrowdStrike and SolarWinds, faulty or manipulated software updates can have cascading, widespread impacts on IT systems.

In our prior work, we’ve identified 7 practices to manage and protect federal IT against these risks. But when we looked at how agencies (23 of them) implemented these practices, [we found](#) that few had. Learn more by listening to our podcast with GAO’s Carol Harris about supply chain risks.

0:00 / 0:00

[Transcript](#)

Many manufacturers of IT products and services are located overseas, which also creates vulnerabilities for the United States. The federal government needs to take action to better monitor the global supply chain against emerging threats. These threats include those against the Department of Defense, which [we reported on in May 2023](#).

**Cybersecurity issues like these are High Risk.
Here’s what needs to happen**

Malicious cyberattacks on the federal government and the nation's critical infrastructures—like that on SolarWinds, and others—are growing in number, impact, and sophistication. This issue is so significant that [in June](#), we updated our High Risk designation for cybersecurity. This update includes descriptions of the major challenges facing the federal government in its efforts to protect against attacks. Some of these challenges are related to the vulnerabilities seen during the CrowdStrike and SolarWinds software updates and responses.

National Cybersecurity Strategy. Last year, the White House issued a National Cybersecurity Strategy outlining steps the government is taking to address the longstanding cybersecurity challenges facing the country. But when [we looked](#) at the strategy, we found it needed outcome-oriented performance measures for its various initiatives.

In addition, the federal government needs to take action to ensure it is monitoring the global supply chain, confirm it has the highly skilled cyber workforce it needs, and address risks associated with emerging technologies—such as artificial intelligence.

We've made nearly 400 recommendations to strengthen the National Cybersecurity Strategy and agencies' ability to perform effective oversight. As of May, 170 of our recommendations have not been acted on.

Critical infrastructure sectors remain vulnerable. Attacks on critical infrastructure sectors continue to grow and could seriously harm human safety, national security, the environment, and the economy. For example, a February attack on Change Healthcare (a health payment processor) resulted in nearly \$874 million in financial losses and widespread disruptions for providers and patient care. Healthcare is just one of the 16 critical infrastructure sectors that are vulnerable to cyberattacks. All of these sectors rely heavily on IT systems to operate.

The 16 Critical Infrastructure Sectors



Sources: GAO analysis of Presidential Policy Directive-21; motorama/stock.adobe.com (icons). | GAO-24-107231

The federal government has taken some steps to address the challenges with protecting these systems from cyberattacks. But we see persistent shortcomings in these efforts. We've made 126 recommendations to better protect the cybersecurity of critical infrastructure. Action is still needed on 64 of them.

Learn more about our work on federal cybersecurity and critical infrastructure protection by reading our [June High Risk update](#) report.

-
- GAO's fact-based, nonpartisan information helps Congress and federal agencies improve government. The WatchBlog lets us contextualize GAO's work a little more for the public. Check out more of our posts at [GAO.gov/blog](https://www.gao.gov/blog).

Topics

Information Security

Information Technology

Cybersecurity and Infrastructure Security Agency

Cybersecurity

Supply chain security

Federal information technology security assessment framework

Information technology

Critical infrastructure

Critical infrastructure protection

Critical infrastructure vulnerabilities

Cyber attacks

Cyber security

Information Technology and Cybersecurity

GAO Contacts



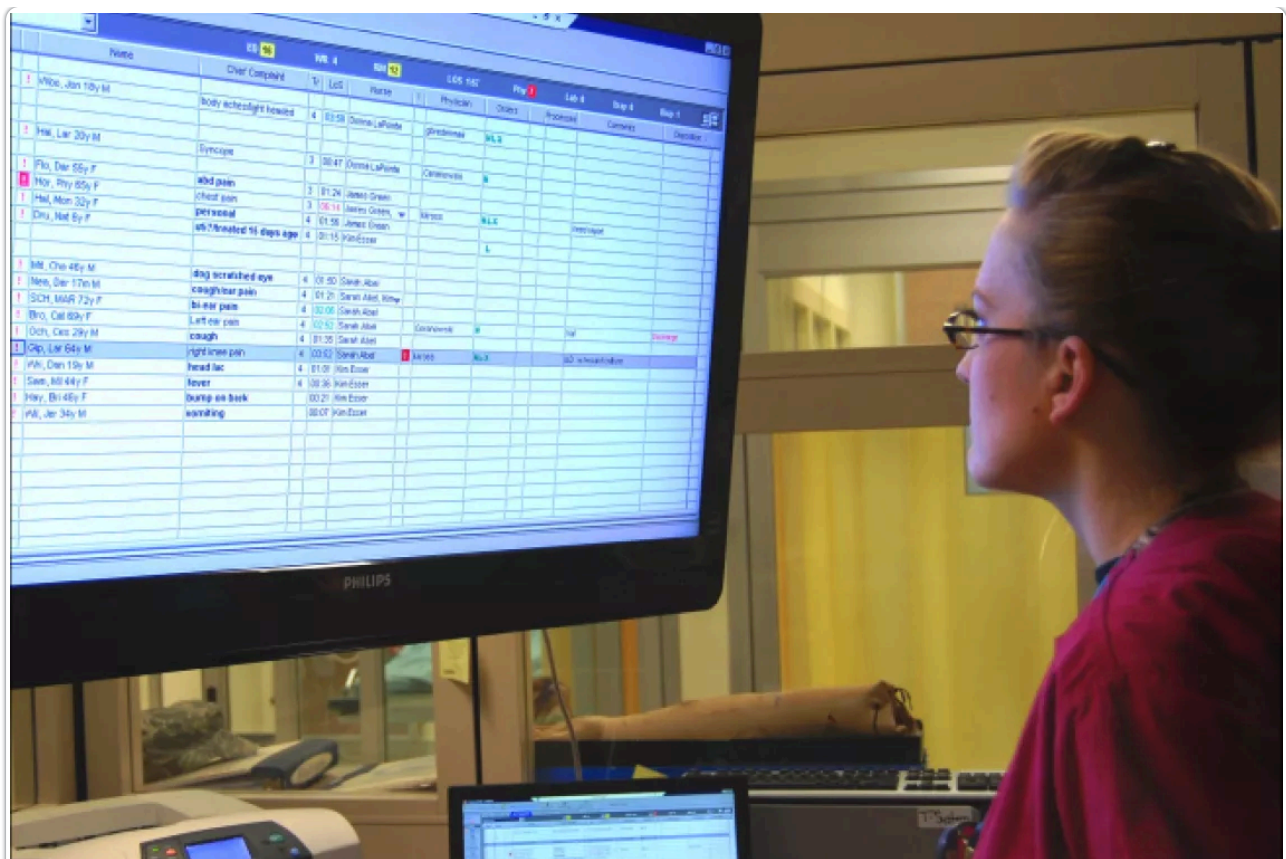
Jennifer Franks

Director

Information Technology and Cybersecurity

✉ franksj@gao.gov

Related Posts

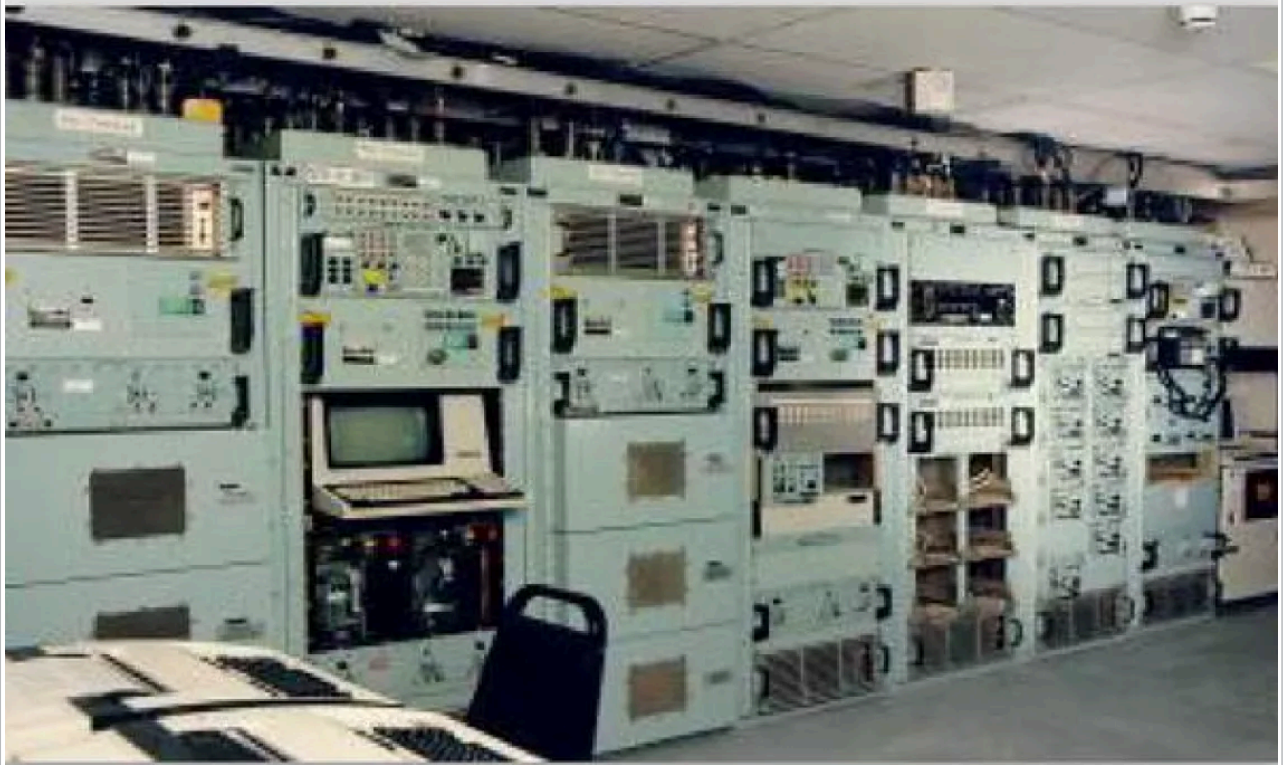


Blog Post

Veterans Affairs' Ongoing Struggle to Modernize Its Electronic Health Record System

TUESDAY, MARCH 18, 2025

After three unsuccessful attempts, the Department of Veterans Affairs is currently on its fourth...



Source: U.S. Department of Defense. | GAO-25-107852

Blog Post

Federal Efforts to Update Old IT are Years Behind Schedule—We Looked at the Impacts of Delays

WEDNESDAY, MARCH 12, 2025

Each year, the federal government spends more than \$100 billion to manage its IT systems, acquire...



Source: i1gend/stock.adobe.com.

Blog Post

The Next Big Cyber Threat Could Come from Quantum Computers... Is the Government Ready?

WEDNESDAY, JANUARY 22, 2025

Whether you're sending an email, paying a bill online, or logging in to a credit card or bank...

Related Products

High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation

GAO-24-107231

Published: Jun 13, 2024

Publicly Released: Jun 13, 2024

Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks

GAO-21-171

Published: Dec 15, 2020

Publicly Released: Dec 15, 2020

Information and Communications Technology: DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks

GAO-23-105612

Published: May 18, 2023

Publicly Released: May 18, 2023



GAO's mission is to provide Congress with fact-based, nonpartisan information that can help improve federal government performance and ensure accountability for the benefit of the American people. GAO launched its WatchBlog in January, 2014, as part of its continuing effort to reach its audiences—Congress and the American people—where they are currently looking for information.

The blog format allows GAO to provide a little more context about its work than it can offer on its other social media platforms. Posts will tie GAO work to current events and the news; show how GAO's work is affecting agencies or legislation; highlight reports, testimonies, and issue areas where GAO does work; and provide information about GAO itself, among other things.

Please send any feedback on GAO's WatchBlog to blog@gao.gov.

Receive GAO Updates

Stay informed as we add new reports & testimonies.

Enter Your Email Address

SUBSCRIBE



U.S. Government
Accountability Office

[Press Center](#)

[Contact Us](#)

[Inspector General](#)

[Restricted Reports](#)

[Copyright & Terms of Use](#)

[Privacy Policy](#)

[Accessibility](#)

[Sitemap](#)

[FOIA Requests](#)

[Scam Alerts](#)

[No FEAR Act Data](#)

[Health Care Advisory Committees](#)