Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 4, 2024

CrowdStrike IT Outage: Impacts to Public Safety Systems and Considerations for Congress

On July 19, 2024, CrowdStrike, a U.S. cybersecurity firm, released a software update to their customers. The update caused certain computer systems to crash, disrupting services across several industries, including airlines, banks, and hospitals, as well as government agencies and public safety systems.

CrowdStrike reported that the incident was caused by "a defect found in a single content update for [Microsoft] Windows hosts" and was not a cyberattack. Though the update affected less than 1% of all Windows machines, the impacts were widespread and global. The incident illustrates the vulnerabilities of information technology (IT) systems, increased dependence and risks in relying on third-party vendors for critical IT services, and lack of protocols and backup systems in the event of IT system failures.

This In Focus discusses the incident's impact on certain U.S. public safety communications systems and services.

Impact on Public Safety Systems

The incident affected public safety agencies that use CrowdStrike's cybersecurity software on their computer systems. This included some 911 systems; police and fire agency systems; fire alarms; and broadcast networks, some of which play a role in emergency alerting. It also affected the computers and operations of some federal agencies that support public safety agencies and emergency response.

Selected 911 Systems and Services

The CrowdStrike update reportedly affected public safety systems and services across several states. In some areas, 911 centers could receive voice calls, but their computer systems were not operational. The following are two examples:

- In Phoenix, AZ, the police department reported that the outage affected their computerized 911 dispatch center. People could still call the 911 center and calls were being answered, but caller information was recorded manually rather than through the computerized dispatch system.

- In Portland, OR, the mayor's office announced that some of the city's computers and servers were affected, including the Bureau of Emergency Communication computer-aided dispatch (CAD) system. People could call the 911 center, but calls had to be answered manually rather than through its computerized system.

In other areas, the update reportedly affected 911 calling. In Alaska, for example, state troopers announced that 911 systems were not operating correctly and posted alternative phone numbers to call in lieu of 911. In Middletown, OH, police notified the public that 911 calls were not being received and offered alternative phone numbers. Other jurisdictions reported no impacts to 911 services.

Other Public-Safety-Related Systems

In some areas, the faulty CrowdStrike update affected other public-safety-related systems. For example, in Columbus, OH, police reportedly were unable to access law enforcement data and license plate information from their in-vehicle terminals, and firefighters were unable to receive dispatch information in their vehicles. In Ocean City, MD, alarms that automatically contact the fire department upon detection of a fire reportedly were affected.

Federal Agencies Supporting Public Safety

Some federal agencies also reported issues following the CrowdStrike update. For example, a Department of Homeland Security (DHS) manager reported that some staff encountered problems logging into desktop computers but were able to work through phones, virtual desktops, or web-based applications. In addition, DHS's Federal Emergency Management Agency (FEMA) reported some issues with its systems but did not identify any impacts to its "critical or immediate lifesaving and life-sustaining operations" or any loss of data. FEMA's Integrated Public Alert and Warning System and the Emergency Alert System were reportedly working normally; however, some broadcasters whose stations may distribute alerts and warnings were affected.

Impact on Telecommunications Systems

Public safety agencies rely on commercial telecommunication networks as an additional means of communications for prioritization of calls for officials and for 911 calling and emergency alerting. Telecommunication networks seemingly were not affected by the incident. People were able to make calls and communicate on landline and cell phone networks. IT systems of some telecom providers who use CrowdStrike's service were affected, leading to some disruption of business operations and customer service, but networks remained operational.

Like the February 22, 2024, outage of the AT&T wireless network, the CrowdStrike incident was caused by a faulty software update and affected public safety systems. However, AT&T was updating its own network, whereas CrowdStrike—a third-party vendor providing cybersecurity services to companies and government agencies—was updating its software on its customers' computers.

Future Public Safety Considerations

In a 2017 white paper on telecommunications security, Oracle, a U.S.-based computer networking technology

company, explained that telecommunication networks were "designed in a different era," where a small set of operators managed the physical interconnection of networks and network security. The emergence of internet protocol (IP)—the set of rules for addressing and routing data over the internet—enabled interconnectivity between many networks, creating the global internet and the ability for IP-based networks and devices to interconnect. With the adoption of IP-based devices (e.g., smartphones, smart TVs), Oracle reports, "now virtually anyone can purchase or gain access" to networks, creating new risks.

The telecommunications and public safety sectors have been migrating to IP-based networks and software-defined networks to enhance network management and performance and enable interconnectivity. One example is Next Generation 911 (NG911), which allows for advanced capabilities, such as text-to-911 and other multimedia communications (e.g., videos), improved call routing, enhanced location finding, and interconnection with other 911 centers. While NG911 enables interconnectivity between 911 centers, enhancing redundancy and resiliency, it also introduces new vulnerabilities, including cyber risks.

Some companies address cyber risks internally, protecting their devices, networks, and data through their own IT solutions, whereas others employ third-party vendors such as CrowdStrike. Use of third-party vendors for critical IT services creates another risk for network operators in that any outage caused by or to a third-party provider or supplier also presents risks. In this case, dependence on CrowdStrike, a large cybersecurity firm that offers its services globally, explains the widespread outage.

The incident demonstrates the need for cybersecurity detection and services as well as the heavy reliance that entities, including public safety agencies, may have on one vendor. The risk is that when the vendor releases a software update over the internet, it can affect many computers and many entities at once, including public safety agencies. As more public safety systems move toward IP-based systems, more entities may rely on network-based, third-party services to address cyber risks. In this context, it may be important for public safety agencies to increase awareness of dependencies and attention to and investment in backup protocols and systems to ensure continuity of service.

Executive Branch Response

The White House reportedly assessed the impact of the incident on federal IT, critical infrastructure, and public safety systems and to industry. DHS's Cybersecurity and Infrastructure Security Agency (CISA) announced that it was working closely with CrowdStrike and with federal, state, local, tribal, and territorial partners, as well as with critical infrastructure and international partners, to assess impacts and support remediation efforts. CISA issued an alert on July 19, 2024, and periodic updates through August 6, 2024. The Federal Communications Commission (FCC) reported that it was working with federal agencies to assist with the disruptions and assess the impact on 911 services.

Congressional Response

Some Members and committees requested and received briefings from CrowdStrike. On July 22, 2024, the chair and a subcommittee chair of the House Committee on Homeland Security requested that CrowdStrike's CEO schedule a hearing with the subcommittee. During the hearing, which was held on September 24, 2024, Members focused on CrowdStrike's actions to prevent a similar attack in the future. In response, a CrowdStrike Senior Vice President said the company has adopted changes in its processes, such as enhanced testing, gradual rollouts of updates, and other safeguards. Members also acknowledged vulnerabilities in interconnected systems. CrowdStrike reiterated the importance of public-private sharing of information on threats and outages, especially to critical infrastructure.

Considerations for Congress

Congress may seek to assess and address new risks and backup considerations for public safety agencies, particularly as it considers funding for the transition to NG911. For instance, Congress could direct DHS's CISA to investigate the incident or to work with public and private partners to identify and assess risks to public safety systems and recommend mitigation methods and best practices to avoid outages of public safety systems. In addition, it could require the National Institute of Standards and Technology to develop recommendations for minimum standards for testing and release protocols for software updates as it does for software testing and security.

Congress could provide or prioritize funding for critical infrastructure, including public safety systems, to assess and address risks, including risks from third-party vendors. Congress could also rely on private sector entities to assess and address risks, such as efforts undertaken by Microsoft for the CrowdStrike outage.

A common complaint during outages has been lack of information and public notice. Congress could consider enhancing outage reporting requirements. While the FCC regulates telecommunications service providers and requires reporting of outages that may affect 911 services, it has limited regulatory authority over internet or IT service providers that interconnect with public safety systems (e.g., 911, alerting). The FCC sought comment on a proposal to require broadband internet service providers to report on outages, citing public safety dependencies on the internet. Congress may consider policies to ensure that internet outages are quickly mitigated and reported in a timely manner to both public safety officials and to the public.

See also CRS Report R48135, *IT Disruptions from CrowdStrike's Update: Frequently Asked Questions*.

Colby Leigh Pechtol, Specialist in Telecommunications Policy
Jill C. Gallagher, Specialist in Telecommunications Policy

IF12717

Disclaimer