

# NetChoice

July 25, 2024

The Honorable Gary Peters  
Chairman  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Rand Paul  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Krysten Sinema  
Chairwoman  
Subcommittee on Government Operations and Border Management  
United States Senate

The Honorable James Lankford  
Ranking Member  
Subcommittee on Government Operations and Border Management  
United States Senate

Dear Senators:

In the wake of what has widely been referred to as the world's largest IT outage in history<sup>1</sup>, we respectfully request the Senate Homeland Security and Government Affairs Committee convene a hearing with both CrowdStrike and Microsoft to examine the steps both companies are taking in order to prevent similar instances in the future.

On July 19, a routine update to CrowdStrike's Falcon Sensor software inadvertently caused widespread disruptions for Microsoft Windows users globally. This update led to critical system failures, including so-called "Blue Screen of Death" errors and boot loops, affecting

---

<sup>1</sup> <https://www.cnn.com/2024/07/19/latest-live-updates-on-a-major-it-outage-spreading-worldwide.html>

approximately 8.5 million devices worldwide. The outages disrupted a wide range of sectors including airlines, emergency room services, financial institutions, and the federal government, which continue to be felt today.

The widespread nature of the outage and its profound impact underscores the urgent need to address the implications of single points of failure in America's critical IT infrastructure. While CrowdStrike's role will be explored in an upcoming hearing in the U.S. House, many questions remain about Microsoft.

The outage made clear that Microsoft software sits at the foundation of many critical industries. According to one estimate, this outage cost businesses \$5.4 billion - yet only affected 1% of Microsoft's systems globally.<sup>2 3</sup>

Just last month, Microsoft Vice Chair and President Brad Smith testified before the House Homeland Security Committee, seeking to reassure lawmakers about steps the company was taking to improve its cybersecurity infrastructure. This occurred after a Cyber Safety Review Board report found systematic weakness in Microsoft's security posture and culture.<sup>4</sup> And while the outage was not a "Microsoft incident," a hearing before your committee would provide valuable insight into what failures led up to the outage and what measures both Microsoft and CrowdStrike are taking to make sure this does not happen again. There could be many causes of a future outage that affects Microsoft software, from a nation-state cyber attack to another botched update, and this incident made clear that any widespread Microsoft outage could bring critical industries and services in our nation to a standstill.

NetChoice has long supported legislation to increase diversification and flexibility in software licensing which can reduce the vulnerabilities inherent in an over-reliance on a single software provider.<sup>5</sup> The over-reliance on a single set of IT systems presents significant risks that can jeopardize an organization's functionality and resiliency and can be mitigated in multi-cloud environments.

---

<sup>2</sup> [We finally know what caused the global tech outage - and how much it cost](#)

<sup>3</sup> [Helping our customers through the CrowdStrike outage](#)

<sup>4</sup> A Cascade of Security Failures: Assessing Microsoft Corp's Cybersecurity Shortfalls and the Implications for Homeland Security  
<https://homeland.house.gov/hearing/a-cascade-of-security-failures-assessing-microsoft-corporations-cybersecurity-shortfalls-and-the-implications-for-homeland-security/>

<sup>5</sup>

<https://netchoice.org/the-samosa-act-promotes-a-more-cost-effective-and-digitally-secure-federal-government/>

The scale of the July 19 outage is unprecedented and will no doubt go down in history. It offers a chilling glimpse of what could occur if, instead of a faulty update, these and other systems were taken down on purpose in a targeted attack by America's adversaries.<sup>6</sup>

We thank you for your consideration of our request. Your attention to this matter is vital for ensuring transparency and strengthening the nation's cybersecurity infrastructure.

Sincerely,

Amy Bos  
Director of State and Federal Affairs, NetChoice

*NetChoice is a trade association that works to protect free expression and promote free enterprise online.*

---

<sup>6</sup> FBI director warns Chinese hackers aim to 'wreak havoc' on U.S. critical infrastructure