COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Ranking Member Bennie G. Thompson (D-MS)

An Outage Strikes: Assessing the Global Impact of CrowdStrike's Faulty Software Update

September 24, 2024

Thank you, Chairman Garbarino and Ranking Member Swalwell, for holding today's hearing on July's CrowdStrike incident, where an error in a content update resulted in an estimated 8.5 million Windows devices crashing.

While this incident was not the result of a malicious cyber attack, it highlighted the risks in our supply chain where a single error by one technology provider can have widespread impacts across critical infrastructure.

Today's hearing is an opportunity to hear directly from CrowdStrike on what went wrong and what steps it is taking to ensure that such mistakes do not happen again.

In an effort to secure technology from cyber attacks, we have deployed technology like CrowdStrike's endpoint detection and response software across government and critical infrastructure networks.

This technology is critical to cyber defense but frequently utilizes significant access to computer networks, creating a risk of incidents like the one that took place in July.

Those companies that sell such technologies must implement best practices to ensure that there are no errors that could disrupt the functioning of critical networks.

This incident also highlighted a significant risk that the Homeland Security Committee discussed at a hearing with Microsoft's President in June—the inherent risks created by vendor concentration.

As we saw on July 19th, CrowdStrike's technology underpins the security of a vast array of companies and government agencies, which allowed an error in one company's technology to have such a significant impact.

In order to reduce the risks of similar incidents going forward, we must ensure we have adequate vendor diversity.

I look forward to working with my colleagues on this Committee to continue our efforts to better understand how vendor concentration impacts risks to critical infrastructure and how the Federal government can ensure its technology acquisition policies do not exacerbate those risks.

I appreciate that Microsoft hosted a summit with security vendors earlier this month on how to improve resiliency and avoid similar incidents in the future.

As we have all become more dependent on technology, the potential for malicious or accidental incidents disrupting critical functions has increased, and reducing that risk will require public-private collaboration on developing best practices and standards.

I am glad that some of that work has begun and look forward to hearing more from our witness today on how CrowdStrike plans to use its experience from this incident to inform broader industry efforts.

As the lead agency for civilian cyber defense, CISA will have a critical role to play in these discussions, and I hope our hearing today will cover how CISA can leverage its expertise and partnerships to better support a more secure and resilient technology ecosystem.

I thank you, Mr. Meyers, for appearing before the subcommittee today and look forward to your testimony.

# # #

Media contact: Adam Comis at 202-225-9978