COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrastructure Protection Subcommittee Ranking Member Eric Swalwell (D-CA)

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

September 24, 2025

I would like to thank Chairman Garbarino for holding today's hearing on the global IT outage that occurred over the summer because of a faulty update by CrowdStrike.

While we are not here today to malign CrowdStrike, we have an obligation to get to the bottom of the circumstances and failures that enabled one content update to crash the operating system of 8.5 million devices worldwide.

The impacts were as diverse as CrowdStrike's customer base: flights were grounded, surgeries were canceled, 9-1-1 dispatch systems were disrupted, and stores had to close.

Parametrix, an insurance company, estimated that 25 percent of Fortune 500 companies were affected and that the incident caused $5.4 billion in losses.

Last year, for the third year in a row, CrowdStrike ranked number one for Endpoint Security market share, with 17.7 percent of the $8.6 billion Endpoint Security Market.

With a market share that size, CrowdStrike must ensure that its product adequately balances the need for access in an operating system against the risks that access poses, and it must consider the lessons learned from similarly situated security firms as it does so.

And with the exceptional level of access it has within a customer's operating system, CrowdStrike has an obligation to employ rigorous quality assurance processes for any updates it releases – even if it is P-code. Neither of those things seemed to happen before the July 19 outage.

I appreciate CrowdStrike's commitment to ensuring its customers are protected against the most novel threats, but speed cannot come at the cost of operability.

At the end of the day, even the best security product on the market won't do any good if it bricks a customer's operating system.

In 2007, a different security firm – Symantec - released a faulty update that also resulted in the dreaded "Blue Screen of Death."

In the aftermath, the company undertook a thorough review of what went wrong, and ultimately implemented a series of changes to both its product architecture and the processes it uses to roll out updates.

Notably, it developed a mechanism to automatically roll-back an operating system to a working state when an error is detected, began releasing updates incrementally, and removed code from the operating system kernel.

As we discuss the July 19th outage today, I will be interested in whether CrowdStrike considered the 2007 Symantec incident as it defined its own processes for testing and releasing updates or defining the level of kernel access it needs to operate.

For the record, this is not the first time this Congress that we have had to ask a technology company why it failed to integrate lessons learned from an incident at a competitor company into its own security practices.

Earlier this year, the Committee held a hearing on a Cyber Safety Review Board report that found that a 2023 compromise of Microsoft Exchange Online mailboxes could have been prevented had it adopted the security controls its competitors implemented following similar incidents that occurred nearly 15 years prior.

One of our goals today is to ensure that we stop re-learning yesterday's lessons so we can more proactively defend against the threats we will face in the future.

Toward that end, I was pleased that earlier this month Microsoft convened the Windows Endpoint Security Ecosystem Summit, which brought together a diverse group of security firms to discuss issues ranging from Safe Deployment Practices to providing additional security capabilities outside of kernel mode.

Today, I hope to get a better understanding of the trade-offs between kernel access and risks to the operating system and learn how we can better manage any risks.

I was also pleased to have the opportunity to speak with CrowdStrike's CEO George Kurtz last week.

He assured me of the company's commitment to making sure nothing like the July 19 outage ever happens again, and he shared updates on the actions CrowdStrike has already taken to address some of the key deficiencies that contributed to it.

# # #

Media contact: Adam Comis at 202-225-9978