AN OUTAGE STRIKES: ASSESSING THE GLOBAL IMPACT OF CROWDSTRIKE'S FAULTY SOFTWARE UPDATE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 24, 2024

Serial No. 118–81

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

60–030 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
THOMAS R. SUOZZI, New York
TIMOTHY M. KENNEDY, New York
LAMONICA MCIVER, New Jersey
YVETTE D. CLARKE, New York

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

CARLOS A. GIMENEZ, Florida
MIKE EZELL, Mississippi
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
MARK E. GREEN, MD, Tennessee *(ex officio)*

ERIC SWALWELL, California, *Ranking Member*
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
LAMONICA MCIVER, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

CARA MUMFORD, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

AN OUTAGE STRIKES: ASSESSING THE GLOBAL IMPACT OF CROWDSTRIKE'S FAULTY SOFTWARE UPDATE

Wednesday, September 24, 2024

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:29 p.m. in room 310, Cannon House Office Building, Hon. Andrew R. Garbarino (Chairman of the subcommittee) presiding.

Present: Representatives Garbarino, Gimenez, Ezell, Lee, Luttrell, Green (ex officio), Carter, Swalwell, and Menendez.

Also present: Representatives Gonzales and Timmons.

Mr. GARBARINO. The Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection will come to order.

The purpose of this hearing is to examine the global IT outage that occurred on July 19 as a result of a faulty software update released by CrowdStrike. Members will seek to gain detailed insights into how the faulty software update was developed, deployed, and what errors lead to the wide-spread global disruption. We will discuss the extent of this outage and how it impacted many key sectors of the economy.

We will also examine how malicious cyber actors have leveraged the global IT outage to conduct malicious activity, including phishing attempts.

I now recognize myself for an opening statement. Just over 2 months ago many essential functions came to a grinding halt. Hospitals saw disruptions in their medical systems, thousands of flights were grounded or canceled world-wide, banks experienced down time and transaction processing, and U.S. Federal Government agencies were temporarily unable to assess certain data.

Shortly after detection we learned that this global IT outage, regarded as the largest in history, was not due to a malicious cyber attack but instead a faulty software update pushed out by CrowdStrike.

According to a company statement, a sensor configuration update triggered a logic error, leading to system crashes and an inability to properly reboot and ultimately the blue screen of death appearing on impacted systems world-wide.

CrowdStrike software updates are essential for addressing vulnerabilities, enhancing threat detection, and ensuring that cybersecurity infrastructure of its customers remains robust as a cyber threat landscape rapidly evolves. Most importantly, given CrowdStrike's value as a resource across the greater cyber ecosystem, these updates are meant to build customer confidence and trust.

We are here today to get answers for our constituents, what went wrong, what was required in response and what we have learned for the future of our Nation's cybersecurity posture. The sheer scale of this error was alarming.

If a routine update could cause this level of disruption, just imagine what a skilled, determined nation-state actor could do. We cannot lose sight of how this incident factors into the broader threat environment. Without question, our adversaries have assessed our response, recovery, and true level of resilience. However, our enemies are not just nation-states with advanced cyber capabilities. They include a range of malicious cyber actors who often thrive in the uncertainty and confusion that arrives during large-scale IT outages.

For example, CISA issued a public statement noting that it had observed threat actors taking advantage of this incident for phishing and other malicious activity. So it is clear that this outage created an advantageous environment ripe for exploitation by malicious cyber actors.

We are joined today by Mr. Adam Meyers who serves as a senior vice president for Counter Adversary Operations at CrowdStrike. Mr. Meyers, I look forward to hearing from your testimony about how a faulty software update was pushed out globally, what CrowdStrike has learned from this event to prevent future outages and how CrowdStrike is working to rebuild trust.

I would also like to discuss the impact this global outage has had on our Nation's various critical infrastructure sectors, what CrowdStrike—what support CrowdStrike has provided to those who were disrupted, and how the company has addressed certain malicious cyber actors who have attempted to take advantage of the global outage. Mr. Meyers, thank you for being here with us today. I look forward to a productive discussion.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

SEPTEMBER 24, 2024

Just over 2 months ago, many essential functions came to a grinding halt. Hospitals saw disruptions in their medical systems, thousands of flights were grounded or canceled world-wide, banks experienced down time in transaction processing, and U.S. Federal Government agencies were temporarily unable to access certain data.

Shortly after detection, we learned that this global IT outage—regarded as the largest in history—was not due to a malicious cyber attack but instead a faulty software update pushed out by CrowdStrike.

According to a company statement, a sensor configuration update triggered a logic error, leading to system crashes, an inability to properly reboot, and ultimately the "blue screen of death" appearing on impacted systems world-wide.

CrowdStrike's software updates are essential for addressing vulnerabilities, enhancing threat detection, and ensuring that the cybersecurity infrastructure of its customers remains robust as the cyber threat landscape rapidly evolves.

Most importantly, given CrowdStrike's value as a resource across the greater cyber ecosystem, these updates are meant to build customer confidence and trust.

We are here today to get answers for our constituents: what went wrong, what was required in response, and what we have learned for the future of our Nation's cybersecurity posture.

The sheer scale of this error was alarming. If a routine update could cause this level of disruption, just imagine what a skilled and determined nation-state actor could do.

We cannot lose sight of how this incident factors into the broader threat environment. Without question, our adversaries have assessed our response, recovery, and true level of resilience.

However, our enemies are not just nation-states with advanced cyber capabilities. They include a range of malicious cyber actors who often thrive in the uncertainty and confusion that arise during large-scale IT outages. For example, CISA issued a public statement noting that it had "observed threat actors taking advantage of this incident for phishing and other malicious activity."

So, it is clear that this outage created an advantageous environment ripe for exploitation by malicious cyber actors.

We are joined today by Mr. Adam Meyers, who serves as the senior vice president of counter adversary operations at CrowdStrike.

Mr. Meyers, I look forward to hearing your testimony about how a faulty software update was pushed out globally, what CrowdStrike has learned from this event to prevent future outages, and how CrowdStrike is working to rebuild trust.

I would also like to discuss the impact this global outage has had on our Nation's various critical infrastructure sectors, what support CrowdStrike has provided to those who were disrupted, and how the company has addressed certain malicious cyber actors who have attempted to take advantage of the global outage.

Mr. Meyers, thank you for being here with us today. I look forward to a productive discussion.

Mr. GARBARINO. I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell for his opening statement.

Mr. SWALWELL. I thank the Chairman. I thank you for convening us here today. Bottom line is, you know, we need CrowdStrike to be effective and successful because its effectiveness and its success is the success of the companies that it protects. So I appreciate CrowdStrike also being a part of this hearing on the global IT outage that occurred over the summer.

While we're not here today to malign CrowdStrike and I don't think you're going see that, you're going to see 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 world-wide. The impacts were as diverse as CrowdStrike's customer base: flights were grounded, surgeries were canceled, 9–1–1 systems were disrupted, and stores had to close. Parametric, an insurance company, estimated that 25 percent of fortune 500 companies were affected and that the incident cost $5.4 billion in losses.

Last year, for the third year in the row, CrowdStrike ranked No. 1 for endpoint security market share, with 17.7 percent of the market and $8.6 billion endpoint security dollars in that market. With a marketshare that size, CrowdStrike must ensure its product adequately balances the need for access in an operating system, against the risks that that access poses. It must consider the lessons learned from this incident as we move forward. With the exceptional level of access that CrowdStrike has within a customer's operating system, CrowdStrike has an obligation to employ rigorous quality assurance process for any updates it releases, even if it is P-Code. We are here to determine if any of these things happened 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 day even the best security product on the market won't do any good if it bricks a customer's operating system. This is not the first time this has happened to a company. It is going to happen; it will happen again.

In 2007, a different security firm released a faulty update that 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. That's the process we want it see happen here.

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 19 outage, I will be interested in whether CrowdStrike considered the 2007 incident as it defined its own processes for testing and releasing updates or defining the level of kernel access it needs it 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 from an incident at a competitor company into its own security practices.

Earlier this year the committee held a hearing on Cybersafety Review Board report that found that a 2023 compromise of Microsoft Exchange on-line could have been prevented had it adopted the security controls its competitors implemented following similar incidents that occurred nearly 15 years prior.

We get better when companies cooperate. Because Microsoft came to that hearing and worked with us and CISA and because CrowdStrike is here today and is working with us and CISA, we will get better. One of our goals is to ensure that we stop relearning yesterday's lessons so we can more proactively defend against the threats that we will face in the future.

Toward that end, I was pleased that earlier this month Microsoft unveiled and convened the Windows Endpoint Security Ecosystem Summit which brought together a diverse group of security firms that discuss issues that range from safe deployment practices, to providing additional security capabilities outside of kernel mode.

Today, I hope to get a better understanding of the tradeoffs between kernel access and risks to the operating system and learn how we can better manage risks. I'm also pleased that last week I had the opportunity to speak with CrowdStrike CEO George Kurtz. He assured me of the company's commitment to making sure nothing like the July 19 incident happens again and shared updates on the actions CrowdStrike has already taken to address some of the key deficiencies that had contributed to it.

Again, Mr. Chairman, I appreciate you holding this hearing and I look forward to seeing what constructive lessons we can learn.

I yield back.

[The statement of Ranking Member Swalwell follows:]

STATEMENT OF RANKING MEMBER ERIC SWALWELL

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 world-wide.

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 No. 1 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 19 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 tradeoffs 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.

Mr. GARBARINO. Thank you, Ranking Member Swalwell.

I now recognize the Chairman of the full committee, a gentleman from Tennessee, Dr. Mark Green, for his opening statement.

Mr. GREEN. Thank you, Chairman Garbarino and Ranking Member Swalwell for your leadership on advancing our Nation's cybersecurity and holding this very important hearing.

On July 19, Americans woke up to a shock: their flight home, grounded; their scheduled medical procedure, canceled; their call to 9–1–1 wouldn't go through. The list goes on. Everywhere Americans turned basic societal functions were unavailable. As Americans looked across our borders they saw other countries, including our allies Australia and the United Kingdom, affected too.

A global IT outage that impacts every sector of the economy is a catastrophe that we would expect to see in a movie. It's something that we would expect to be carefully executed by malicious and sophisticated nation-state actors.

To add insult to injury, the largest IT outage in history was due to a mistake. In this case, CrowdStrike's content validator used for its Falcon Sensor did not catch a bug in a channel file.

It also appears that the update may not have been appropriately tested before being pushed out to the most sensitive part of the computer's operating system. This caused about 8.5 million devices to crash.

Mistakes happen; however, we cannot allow a mistake of this magnitude to happen again. As the July 19 outage has demonstrated yet again our networks are increasingly interconnected. While we know that the nation-state actors and criminals try to exploit our networks we would not expect companies to defend themselves from these targeted attacks.

However, as I emphasized with the president of Microsoft in June, we do expect companies to implement the strongest cybersecurity practices. Our Nation's security depends on a strong public-private partnership for protecting our networks.

Ensuring our partnership is strong is important because our adversaries always watch how we respond to these type of incidents, just like the July 19 outage. You can bet they are watching us right now.

The good news is that since this was not due to a cyber attack, we can learn from the incident. Today's hearing is both timely in one way and overdue in another. Timely because we now have 2 months of information to understand exactly what happened and I'm hopeful this will make for a very productive hearing. It's overdue because we had hoped to give Americans the answers they deserve much sooner, given the extent of this outage.

Although I'd hoped to hear from CrowdStrike's CEO directly, I'm grateful for Mr. Meyers' presence. I'm confident he will deliver the answers we need. Thank you, Mr. Meyers, for taking the time to walk us through the course of events leading up to July 19 and the steps CrowdStrike has taken since.

In August, CISA director Jen Easterly described this incident as, "a useful exercise, a dress rehearsal for what China may want to do with us." We look forward to working with you to make sure we never make it to opening night.

I yield back my time, Chairman Garbarino.

Mr. GARBARINO. The Chairman yields back.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

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 wide-spread 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 19, 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.

Mr. GARBARINO. I am pleased to have Mr. Adam Meyers before us today to discuss this very important topic. I ask that our witness please rise and raise his right-hand.

[Witness sworn.]

Mr. GARBARINO. Let the record reflect that the witness has answered in the affirmative. Thank you, please be seated.

I would now like to formally introduce our witness. Mr. Adam Meyers currently serves as the senior vice president of counter adversary operations at CrowdStrike. In this role Mr. Meyers leads the threat intelligence line of business for the company. He is responsible for tracking criminal, state-sponsored, and national cyber adversary groups around the world.

He provides technical and strategic guidance for Fortune 100 organizations, Government agencies on how to stay protected and prevent damage from sophisticated, instructive cyber threat actors.

Prior to joining CrowdStrike, Mr. Meyers was a director of cybersecurity intelligence at SRA International. During his tenure he provided technical expertise and strategic guidance for both the commercial sector customers, as well as civilian, military, and intelligence customers. He conducted the penetration test, vulnerability research in a brief investigation across the globe, traveled extensively throughout Africa and South and Central America supporting customers.

Mr. Meyers is a key technical lead supporting the U.S. Department of State Cyber Threat Analysis Division, leading a team of reverse engineers and instant response experts and representing the division at intergovernmental meetings on cyber threats. I thank the witness for being here today.

I now recognize Mr. Meyers for 5 minutes to summarize his opening statement.

STATEMENT OF ADAM MEYERS, SENIOR VICE PRESIDENT, COUNTER ADVERSARY OPERATIONS, CROWDSTRIKE

Mr. MEYERS. Chairman Green, Chairman Garbarino, Ranking Member Thompson, Ranking Member Swalwell, Members of the subcommittee. Good afternoon and thank you for having me here today. I'm Adam Meyers, senior vice president for counter adversary operations at CrowdStrike.

At CrowdStrike our vision is to protect good people from bad things. We've been very successful at doing that for more than a decade. I'm proud to lead the threat intelligence side of our business. I direct a team of cyber threat experts tracking criminal, state-sponsored and cyber adversary groups across the globe. Our goal is to produce actionable intelligence to protect our customers.

Despite our strong track record, I'm here today in part because just over 2 months ago on July 19, we let our customers down. CrowdStrike was in the process of updating our customers on a new threat or at least a content configuration update for the Windows Sensor did not work as expected. This resulted in Microsoft system crashes for a number of our users.

On behalf of everyone at CrowdStrike, I want to apologize. We're deeply sorry. We are determined to prevent this from ever happening again.

We appreciate the incredible round-the-clock efforts that our customers and partners who are working alongside our teams mobilized immediately to restore systems. We were able to bring many customers back on-line within hours. I can assure you that we continue to approach this with a great sense of urgency. I want to underscore that this was not a cyber attack. The incident was caused by a CrowdStrike rapid response content update was focused on addressing new threats.

CrowdStrike began working with customers and partners to bring systems on-line as quickly as possible, initially through manual remediation. CrowdStrike then introduced automated techniques to accelerate remediation. To further help customers bring systems on-line as quickly as possible CrowdStrike also put boots

on the ground, to assist customers with recovery efforts. We also provided regular updates to customers throughout our response, these are available on our website and have been shared with policy makers and our customers.

We've also taken numerous steps to make sure this can't happen again. We are pleased to report that as of 29 July, approximately 99 percent of Windows sensors were back on-line.

We have endeavored to be transparent about what happened and are committed to learning from what took place. We have undertaken a full review of our systems and are implementing plans to bolster our content, update procedures so that we emerge from this experience as a stronger company. I can assure you that we will take the lessons learned from this incident and use them to inform our work as we improve for the future.

Finally, as we have enhanced our own resiliency we remain laser-focused against disruptive cyber attacks as we have for a decade. While we have fixed the issue that led to this incident, there are many other threats that remain on the horizon. The threat environment is particularly challenging, given global unrest and the upcoming election here in the United States. We are focused on threats from nation-state adversaries, issue-motivated hacktivists and sophisticated e-crime adversaries motivated by profit. At CrowdStrike we are particularly focused on threats from North Korea, Iran, China, and Russia. Recent events have also highlighted the often underappreciated supply chain security considerations.

Additionally, in the e-crime sphere ransomware means a chronic problem targeting victim organizations across the globe. We appreciate your leadership on these issues and I hope we can discuss some of these arising threats with you today.

Like you, we recognize the importance of remaining vigilant. I'm especially grateful to you and your staff for being accessible over these past several weeks to receive briefings and updates from our team and myself. I look forward to our continued discussion here today.

Thank you and I welcome your questions.

[The prepared statement of Mr. Meyers follows:]

PREPARED STATEMENT OF ADAM MEYERS

SEPTEMBER 24, 2024

Chairmen Green and Garbarino, Ranking Members Thompson and Swalwell, Members of the subcommittee: Good afternoon and thank you for having me here today. I am Adam Meyers, senior vice president for counter adversary operations at CrowdStrike.

At CrowdStrike, our vision is to protect good people from bad things, and we have been very successful at doing that for more than a decade. I am proud to lead the threat intelligence side of our business. In my role, I direct a geographically-dispersed team of cyber threat experts tracking criminal, state-sponsored, and cyber adversary groups across the globe. My team's goal is to produce actionable intelligence and leverage it to protect our customers from malicious cyber behavior and stop increasingly sophisticated adversaries.

Despite our strong track record in these areas, I am here today because, just over 2 months ago, on July 19, we let our customers down. As part of regular operations, CrowdStrike released a content configuration update for the Windows sensor that resulted in system crashes for many of our customers.

On behalf of everyone at CrowdStrike, I want to apologize. We are deeply sorry this happened and are determined to prevent it from happening again. We appre-

ciate the incredible round-the-clock efforts of our customers and partners who, working alongside our teams, mobilized immediately to restore systems and bring many back on-line within hours. I can assure you that we continue to approach this with a great sense of urgency.

More broadly, I want to underscore that this was not a cyber attack from foreign threat actors. The incident was caused by a CrowdStrike rapid response content update. We have taken steps to help ensure that this issue cannot recur, and we are pleased to report that, as of July 29, approximately 99 percent of Windows sensors were back on-line.

Since this happened, we have endeavored to be transparent and committed to learning from what took place. We have undertaken a full review of our systems and begun implementing plans to bolster our content update procedures so that we emerge from this experience as a stronger company. I can assure you that we will take the lessons learned from this incident and use them to inform our work as we improve for the future.

I look forward to our discussion today about what happened, our subsequent diligent focus on restoring customer systems, and what we have done to enhance our processes since.

CROWDSTRIKE AND THE FALCON PLATFORM

CrowdStrike was built on the principle of applying the Observe, Orient, Decide, Act ("OODA") loop methodology, originally developed for military combat operations. This approach emphasizes the critical importance of speed in cybersecurity, where the ability to quickly observe threats, orient to the changing landscape, decide on a course of action, and execute that action faster than the adversary is paramount.[1] CrowdStrike leverages this methodology to protect 538 Fortune 1000 companies, 298 Fortune 500 firms, and 43 of 50 U.S. States from sophisticated nation-state, hacktivist, and criminal threat actors.[2]

CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes, and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of risk—endpoints and cloud workloads, identity, and data—to keep customers ahead of today's adversaries and stop breaches. We have done attribution on attackers hiding in the shadows; we have disrupted ransomware attacks and high-risk intrusions at thousands of companies; and we have identified and blocked nation-state adversaries seeking to exfiltrate valuable intellectual property globally.

In today's rapidly-evolving threat landscape, the need for dynamic security measures is critical. Adversaries continue to employ increasingly sophisticated techniques to target and infiltrate systems at various stages. We have unfortunately seen a drastic rise in the malicious technologies deployed by bad actors, and the complexity of attacks continues to increase as a reaction to defenders' postures. My particular work at CrowdStrike is focused on ensuring the smooth and speedy integration of intelligence into our entire line-up of products and services to help prevent and detect threats.

The concept of "community immunity" from the public health world applies directly to cybersecurity. As more organizations join the CrowdStrike network, the collective security of all customers improves. Each customer—even each endpoint—contributes additional context and visibility, making the system smarter and faster in detecting and mitigating threats. This network effect means that every participant, including those in especially targeted industries, enhances the security of the entire CrowdStrike community, creating a powerful defensive ecosystem that benefits all. As this network includes trillions of events per day derived from the global footprint of threats detected in technology, telecommunications, financial, government, retail, manufacturing, health care, services, education, media, and more, customers of all sizes benefit from sophisticated protection. Simply put, a thwarted breach for one customer provides a new line of defense for all customers.

Powered by the CrowdStrike Security Cloud, our Falcon Platform leverages real-time indicators of attack, threat intelligence on evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities—all through a single, lightweight agent.

---

[1] Falcon operates at global, cloud-scaled speeds to detect and contain threats before adversaries can escalate their attacks, effectively managing "breakout time."

[2] As of April 30, 2024.

THE JULY 19 INCIDENT: WHAT HAPPENED?

CrowdStrike's Falcon platform is a cloud-native, AI-powered platform that protects customers with a combination of cloud (the CrowdStrike Security Cloud) and on-device security (the Falcon sensor). The CrowdStrike Security Cloud regularly communicates with Falcon sensors installed on customers' end points, such as laptops, desktops, and servers. The Falcon sensor leverages AI, detection, and prevention engines. The detection engine includes the ability to collect threat-related data by following a predefined set of configurations. New configurations are regularly sent to the sensor's detection engine to help protect customers against emerging threats, such as malicious code, ransomware, and data breaches. These threat detection configurations are validated before being sent to the Falcon sensor. Upon receiving new configurations, the Falcon sensor follows a predefined set of rules to enhance detections.

On July 19, 2024, new threat detection configurations were validated through regular validation procedures and sent to sensors running on Microsoft Windows devices. However, the configurations were not understood by the Falcon sensor's rules engine, leading affected sensors to malfunction until the problematic configurations were replaced.

WHY DID IT HAPPEN?

CrowdStrike maintains rigorous testing and validation throughout its entire software development and configuration information creation processes. As part of these testing and validation processes, CrowdStrike's software code is certified by Microsoft through the Windows Hardware Quality Labs ("WHQL") program and tested through a quality assurance process. Configurations read by the code are validated to conform with the expected input specification. While code is updated less frequently, new configurations are sent with rapid occurrence to protect against threats as they evolve.

On July 19, 2024, using a longstanding, routine process, we updated threat detection configuration information leveraged by the sensor, without needing to update the sensor's code. As we describe in detail in our Technical Root Cause Analysis, the July 19 incident stemmed from a confluence of factors that ultimately resulted in the Falcon sensor attempting to follow a threat detection configuration for which there was no corresponding definition of what to do.

1. Validation.—Our validation and testing processes in use for the past decade did not catch this unexpected discrepancy. These validation checks missed this specific scenario, which had not occurred before: a mismatch between input parameters and predefined rules.

2. Testing.—During the development and testing phases, the scenarios tested did not include cases where the final input parameter contained a new configuration that needed a corresponding rule.

3. Input.—The Falcon sensor's rules engine was designed to receive a specific number of inputs and take corresponding actions based upon configurations. Each input would lead to a specific threat detection action defined by the rules. One of the configurations sent on July 19, 2024, contained an extra input for which there was no defined action. This mismatch led the software to follow a configuration without knowing which rules to follow, triggering a malfunction.

OUR SUPPORT FOR CUSTOMERS IN THE WAKE OF THE INCIDENT

CrowdStrike began working with customers and partners to bring systems on-line as quickly as possible, initially through manual remediation. These efforts enabled the systems to come back on-line within hours following the initial incident.

On July 22, 2024, CrowdStrike introduced automated techniques to accelerate remediation.

To further help customers bring systems on-line as quickly as possible, CrowdStrike deployed personnel and engaged with strategic partner services teams to assist customers with recovery efforts. We also worked to provide continuous and transparent updates to customers throughout our response. As of July 29, virtually all of our customers' systems were back up and running.

ENHANCEMENTS TO HELP ENSURE THIS WON'T HAPPEN AGAIN

We have successfully deployed critical detection and preventions over the past decade, validated and tested by our processes, to protect organizations against millions of threats from sophisticated adversaries without such an incident. Since July 19, 2024, we have implemented multiple enhancements to our deployment processes to make them more robust and help prevent recurrence of such an incident—with-

out compromising our ability to protect customers against rapidly-evolving cyber threats.

1. Validation.—We have introduced new validation checks to help ensure that the number of inputs expected by the sensor and its predefined rules match the same number of threat detection configurations provided. This is designed to prevent similar mismatches from occurring in the future.

2. Testing.—We have enhanced existing testing procedures to cover a broader array of scenarios. This includes testing all input fields under various conditions to detect potential flaws before rapidly-released threat detection configuration information is sent to the sensor.

3. Customer Control.—We have provided customers with additional controls over the deployment of configuration updates to their systems.

4. Rollouts.—Our threat detection configuration information, known as Rapid Response Content, is now released gradually across increasing rings of deployment (See Appendix). This allows us to monitor for issues in a controlled environment and proactively roll back changes if problems are detected before affecting a wider population.

5. Safeguards.—We have added additional run-time checks to the system, designed to ensure that the data provided matches the system's expectations before any processing occurs. We are also working to further enhance our safeguards for validation and quality assurance, including by implementing more granular controls.

6. Third-Party Reviews.—We have engaged 2 independent third-party software security vendors to conduct further Falcon sensor code and end-to-end quality control and release processes reviews.

EMERGING THREATS TO RESILIENCY POSED BY ADVERSARIES

As we have enhanced our own resiliency, we remain steadfast in our commitment to continuing to protect our customers against disruptive cyber attacks as we have for a decade. In doing so, we must remain vigilant against cyber threats on the horizon.

Advancements in threat detection, prevention, and response capabilities have aided defenders in recent years, but adversaries have responded by increasingly adopting and relying on techniques to evade detection. This includes supply chain attacks, insider threats, and identity-based attacks. Threat actors' speed also continues to accelerate as adversaries compress the time between initial entry, lateral movement, and "actions of objective" (like data exfiltration or attack). At the same time, the rise of generative AI has the potential to lower the barrier of entry for low-skilled adversaries, making it easier to launch attacks that are more sophisticated and state-of-the-art.

These threats include nation-state adversaries, issue-motivated "hacktivists," and sophisticated eCrime actors motivated by profit. China-nexus adversaries, for instance, have continued to operate at an unmatched pace across the global landscape, leveraging stealth and scale to collect targeted group surveillance data, strategic intelligence and intellectual property. In other areas of the world, conflict has continued to drive nation-state and hacktivist adversary activity. In 2023, as the Russia-Ukraine war entered its second year, Russia-nexus adversaries and activity clusters maintained high, sustained levels of activity in support of Russian Intelligence Service ("RIS") intelligence collection, disruptive activity, and information operations (IO) targeting Ukraine and NATO countries. Iran-nexus adversaries and Middle East hacktivist adversaries were also observed pivoting cyber operations in the latter half of last year in alignment with kinetic operations stemming from the 2023 Israel-Hamas conflict. And North Korean adversaries maintained a consistently high tempo throughout 2023. Their activity continued to focus on financial gain via cryptocurrency theft and intelligence collection from South Korean and Western organizations, specifically in the academic, aerospace, defense, government, manufacturing, media, and technology sectors. In the eCrime sphere, ransomware remains a chronic problem targeting victim organizations across the globe.

OUR ON-GOING COMMITMENT TO OUR PARTNERS AND CUSTOMERS

Nothing is more important to CrowdStrike than the trust and confidence that our customers and partners have put into our company and its products as we continue our mission to stop breaches. We have long focused on protecting the resiliency of critical organizations and infrastructure against sophisticated adversaries. Going forward, we will build upon our long-standing contributions to cybersecurity by continuing to share our lessons learned on ecosystem resiliency.

Thank you, and I look forward to your questions.

APPENDIX

Mr. GARBARINO. Thank you, Mr. Meyers.

Members will be recognized by order of seniority for their 5 minutes of questioning. Initial round of questioning may be called after all Members have been recognized. I now recognize the Chairman of the full committee, the gentleman from Tennessee, Dr. Green, for 5 minutes of questioning.

Mr. GREEN. First let me say, thank you for your statement. There was a degree of humility there that is impressive and I appreciate the transparency that we have seen. I think some of the biggest lessons we learn are in times of adversity and you guys have shown the right attitude so thank you.

In terms of the update, you know, people are really important to me in the cybersecurity—the cybersecurity work force is my No. 1 issue. I mean, I just pushed a bill yesterday that will hopefully address the big shortage that we have across the country. But who

made the decision to launch the update? Did AI do that or did an individual do that? Can you tell me how that decision was made?

Mr. MEYERS. Thank you for your question and your comments.

AI was not responsible for the handy decision in that process. It is part of a standard process. We released 10 to 12 of these updates, content updates every single day. So was part of our standard operating procedure.

Mr. GREEN. These updates are automatic globally? They go global all at once when you send an update out?

Mr. MEYERS. The updates were distributed to all customers in one session. We've since revised that.

Mr. GREEN. OK.

Mr. MEYERS. In the full testimony I've included a graphic that depicts——

Mr. GREEN. OK.

Mr. MEYERS [continuing]. What that now looks like and that is no longer the case.

Mr. GREEN. OK. So we're not—so CrowdStrike is no longer fielding your updates like that, simultaneous universally, if I understood the answer to your question. OK, good.

Honestly that was probably my biggest question, Chairman Garbarino, was to just see that that single fix was in. That's huge. I think it would have prevented what happened from happening. You take, like, how American Airlines I think their router systems were different and it prevented part of their systems from going down and some of their systems did. Whereas other airlines, it went universal and they wound up with more catastrophic outcome, but I'm glad to hear that you guys decided to stair step that update implementation.

I don't really have any other questions, that was my biggest concern so I yield.

Mr. GARBARINO. The Chairman yields back.

I now recognize the gentleman from Louisiana, Mr. Carter for 5 minutes of questions.

Mr. CARTER. Thank you, Mr. Chairman. Thank you, Ranking Member. Thank you to our witness for joining us today.

Cybersecurity protection means securing a network overall for better security and resilience. Despite our annual investment of over $60 billion in cybersecurity, we continue to face significant shortages of trained personnel. This reality underscores a critical point, none of our protective measures be they standards, technologies, or regulations can succeed without a well-trained work force. Addressing on-going and emerging cyber challenges is critical to our Nation's security. Today's discussion is important and thank you for being here.

One contributing fact to the wide-spread impact of the incident that brings us here was the inability of customers to control when they received this kind of update. If customers have the ability to schedule the receipt of updates, is it possible that fewer devices would have—it's possible that fewer devices would have been in fact impacted. I'm pleased that CrowdStrike has addressed this issue and given customers greater control over when they receive content updates. Can you elaborate on what kind of options customers now have with regards to receiving these updates? How are

you ensuring that customers understand the ability to control content update?

Mr. MEYERS. Thank you for your question, Congressman.

Moving forward and what we've implemented is a system of concentric rings think of it. The initial internal release process will be the first step in releasing new content updates. From there, customers can select to be part of the early adopter program where they can choose to receive content updates as quickly as we can make them available. From there, there's another factor that they can select which would be general availability which would come after early adopter. Then from there they can select to wait some period of time before those updates get pushed out or choose not to receive them as well.

Mr. CARTER. Is there a preferred process which if any is safer, more efficient, would grant the greatest amount of honorable protection to the consumer?

Mr. MEYERS. Thank you, Congressman.

I think the early adopter is appropriated for systems for testing purposes. In other words, if an organization would like to receive those content updates in a timely manner and make sure that there is no outcome or unexpected behavior and then from there the general availability. For mission-critical systems or things that they would prefer to wait even longer for, they can choose to do that. But that comes of course with the risk that they are not getting the most up-to-date threat intelligence information provided to their system.

Mr. CARTER. Is there a capacity to overrule those options and to automatically push forward an update because of the sensitivity of the risk?

Mr. MEYERS. From the CrowdStrike side?

Mr. CARTER. Yes.

Mr. MEYERS. No, sir.

Mr. CARTER. OK. Given the revelations that we've had, is there a mechanism for there to be a greater amount of cooperation between CrowdStrike, Microsoft, and the other good actors as opposed to the bad actors who seem to have a leg up in being nefarious, are there mechanisms that you guys have in place that you're coordinating and working more closely in sync to prevent these type of issues the future?

Mr. MEYERS. That's a great question, Congressman. Yes, we've—in fact, on the weekend of July 19 we began working very closely with Microsoft in order to ensure that our mutual customers had the benefit of us working together. Then subsequent to that just last week there was a meeting in Microsoft that was I think already mentioned where CrowdStrike and others participated in a sit-down with Microsoft to plan for future improvements and to ensure continued resiliency by CrowdStrike, Microsoft, and other companies as well.

Mr. CARTER. Last, before my time runs out, is there a mechanism for the community to be made more aware in a kind-of a laymen's sense of what can citizens do to better protect themselves and to be aware? We know there are all kinds of phishing scams, all kinds of stuff out there. What could a general consumer and

what might we be dong as a committee help educate the general public?

Mr. MEYERS. Thank you. Awareness is a key factor as you point out. During this incident we were able to push out threat intelligence on our blogs in order to advise general consumers of threat actors that were trying to take advantage of these situations. In general I think better awareness of these threats is absolutely critical and something that I would be happy to in continue to work with you and your staff on to come up with strategies to help educate the public about some of these threats.

Mr. CARTER. Thank you. My time has expired. I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentleman from Mississippi, Mr. Ezell, for 5 minutes of questions.

Mr. EZELL. Thank you, Mr. Chairman.

The global outage we experienced in July 19, 2024 impacted millions of people and has estimated it cost billions of dollars. This disruption impacted a wide range of services, including airlines, hospitals, emergency service, call centers, and more impacting our Nation and the global economy.

While I appreciate how quickly CrowdStrike identified and deployed a fix to the problem, it turned out that the solution was a minimal reboot process. With workers in rural areas like many communities in Mississippi this means it could have taken them days to find the right IT person to get to the scene and get the computers up and running.

Mr. Meyers, why was that the only solution is a manual fix?

Mr. MEYERS. Thank you for your question, Congressman. Initially there was a manual hands-on process that was required, which we mobilized our entire team to support. We activated our partners, we worked around the clock. I offered myself to drive 10 hours to visit a customer to help them get some of their systems back on-line. Within the next day or so, we were able to identify some automated systems that would enable us to facilitate the recovery at a much faster pace and that was where the bulk of that recovery occurred. We saw a massive uptick in systems coming back on-line once we deployed the automated process.

Mr. EZELL. What steps are you taking to protect your systems from difficult recovery process if something like this happens again?

Mr. MEYERS. Thank you, Congressman.

We as—in the testimony, I referred to this earlier, provided a new system to ensure that the content updates have an opt-in and kind-of the ability to choose when you receive those updates. Prior to this our sensor packages, all of our source code had those established best practices already in place. Now we're applying this as well to the content updates.

Mr. EZELL. I represent south Mississippi. Can you please describe the support CrowdStrike offered or provided to rural communities such as in my district?

Mr. MEYERS. I will need to get back to you with some details of that, sir.

Mr. EZELL. OK. A recent article stated and I quote, "Engineers and threat hunters were given just 2 months for work that would

have normally taken a year." Additionally, the article noted that CrowdStrike confirmed its use of and again I quote, "existing engineers, instead of hiring a new team of cloud threat hunters." Pearl River Community College and many others in my district offer an excellent cybersecurity technology program for our next generation of students to help fill this unsettling skills gap. Do you make these staffing decisions because of lack of adequate job force in the industry?

Mr. MEYERS. Thank you, sir. We have a robust internship program. We bring some of the most—a lot of our talent from these internal and external internship programs and recruit from all over the country and all over the world in order to fill positions.

Mr. EZELL. What steps are you taking to better support your staff and ensure that they have the right tools and skills to succeed?

Mr. MEYERS. That's a good question, sir. We have extensive internal training programs. We also send our team to various trainings across the globe, different industry trainings at conferences and other programs where they can learn new skills and continue to develop their existing schools. Then we also have some of our own researchers analysis conduct trainings at those same events to help train individuals that are not yet in the work force or working at other companies in order to learn some of the critical skills that are needed to identify and to track advanced threat actors.

Mr. EZELL. Mr. Meyers, we know that there are many single points of failure in our cyber ecosystem, these can be exploited either through a mistake or an attack and cause an impact similar to what we saw from the CrowdStrike incident. Additionally, when products are modified or updated, another single point of failure is created. What do you suggest this committee focus on to mitigate single points of failure and improve the stability of these symptoms?

Mr. MEYERS. That's a tough question. I think there's a lot that needs to be done in order to identify and mitigate simple points of failure. We have been acting at CrowdStrike in terms of identifying vulnerable systems across the globe doing research to try to determine where vulnerabilities may exist and come up with mitigating strategies for that. It's a continuing effort, it's something that takes everybody, it's a team sport and we all need to work together for that.

Mr. EZELL. Thank you. Mr. Chairman, I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the Ranking, the gentleman from California, Mr. Swalwell, for 5 minutes of questions.

Mr. SWALWELL. Mr. Meyers, CrowdStrike released its content configuration update into the kernel, which is the core part of the operating system where an error will crash the entire system rather than just one single application. Some competitors of yours have claimed that this kind of kernel access is dangerous and that a better practice is to deploy such updates directly to the user mode where the impacts would only affect an application. Can you explain just for folks who may not understand the kernel in this dialog why CrowdStrike issues updates to the kernel? How it balances

the benefits of kernel access to the risk that it creates? Is CrowdStrike planning to make any changes to how it uses kernel access to reduce the risk crashing entire systems?

Mr. MEYERS. Thank you, Congressman.

The Windows kernel is—and all operating systems have a kernel—this is the central kind-of most part of the operating system, in many cases you'll hear it referred to as ring zero. The kernel is responsible for interfacing with all of the hardware associated with that operating system or that computer. CrowdStrike is one of the many vendors out there that uses the Windows kernel architecture, which is an open kernel architecture. This is a decision that was made by Microsoft to enable Microsoft operating system to support a vast array of different types of hardware and different systems.

The kernel is responsible for the key area awaking, ensure that you have performance where you can have visibility into everything happening on that operating system, where you can provide enforcement. In other words, threat prevention. As well to ensure anti-tampering, which is a key concern from a cybersecurity perspective. Anti-tampering is concerning because when a threat actor gains access to a system they would seek to disable security tools. In order to identify that that's happening, kernel visibility is required to see when that's occurring.

The kernel driver is a key component of every security product that I can think of, whether they would say that they do most of their work in the kernel or not, varies from vendor to vendor, but to try to secure the operating system the without kernel access would be very difficult.

Mr. SWALWELL. The Cyber Safety Review Board has demonstrated that if you conduct a meaningful review of cyber incidents, including the most Microsoft review, which has proven helpful to this committee's oversight of recent incidents involving Microsoft. Some cybersecurity exerts have called for the CSRB to conduct a review of this incident. Do you believe they should? Second if they do, will you fully cooperate with that review?

Mr. MEYERS. Thank you, sir. We would fully cooperate with everything we've been working with CISA, the various ISAT communities and many of your staffs directly since the 19 July incident in order to ensure that we have provided transparency and visibility into everything that's occurring.

Mr. SWALWELL. Shifting toward your mission of protecting your customers and we have seen over the years that our adversaries, particularly around even years in the fall like to weaponize their own capabilities to attack democracy. Can you just give us a picture of the threat environment right now, as far as what you're seeing from our adversaries, any new, unique lines of attack, any particular countries that you see escalating their attacks as we head to November 5?

Mr. MEYERS. Thank you, Congressman.

Our adversaries watch these elections very closely. We've already seen in this election process that Iran has played a role in targeting campaigns. We continue to see China and others as well.

With regard to what activity we've seen thus far, espionage continues to be the primary motivator for countries like China and Russia. We have seen certainly in the past that these adversaries

have stolen sensitive information and leaked them. We also see a rich array of disinformation and misinformation occurring as result of foreign adversaries using social networks and things of that nature to drive narratives that are supportive of their agendas.

Mr. SWALWELL. I yield back.

Mr. GARBARINO. The gentleman yields back.

I new recognize the gentlelady from Florida, Ms. Lee, for 5 minutes for questions.

Ms. LEE. Thank you, Mr. Chairman.

Mr. Meyers, your root cause analysis attributed this global IT outage to a failure in your validator tool. However, it seems like another important contributing factor here was closely related to how you released the software update. So I'd like to go back to the topic of a phased rollout approach. I believe you were describing this change when you used the phrase concentric circles. Starting here, was this update pushed out in a phased way?

Mr. MEYERS. Thank you for the question, Congresswoman.

To be—first, let me state that the configuration update that occurred, the content update was not code. This was threat information that was being provided to the sensor. The code is pushed out and that is the sensor itself—had been pushed out using a phased deployment methodology where the code would go through extensive quality assurance and quality checks. It would then be deployed internally in what we would call dogfooding. Then from there, it would be rolled out to customers who could select N plus—n–1, n–2, meaning they could wait some set period of time before they would actually roll out the new sensor. This sensor was rolled out in February 2024. The content updates are not code. They had not previously been treated as code because they were strictly configuration information.

What we have undertaken since the July 19 incident, what I referred to earlier in the testimony, is it that we are now treating the content updates as code, which is something that I don't believe to be an industry standard at this time. By us treating that as code it is now going through that process of again, the internal testing, dogfooding before it goes to early adopters, general availability and the n minus x strategy.

Ms. LEE. Thank you for that distinction.

Would you agree that in this case while it may have been content update, clearly the failure to have it implemented or take effect in a phased approach ended up being catastrophic.

Mr. MEYERS. We've moved to a phased approach as a result of the incidents of July 19 and we have put a lot of time and effort into making sure that that phased approach will ensure customers have the ability to choose when and how they receive those updates.

Ms. LEE. Going back to the Ranking Member, in his comments you two were discussing the fact that CrowdStrike has really extraordinary access into the kernel of the operating system. You all were taking a bit about the risk versus efficiency of having this kind of access and making updates within the kernel. Share with me your thoughts on whether this incident could have been averted or future incidents could be averted by using the user space for this kind of update.

Mr. MEYERS. Thank you for the question.

The kernel, as I said, provides the visibility, the enforcement mechanism, the telemetry and visibility—as well as the anti-tamper. So I would suggest that while things can be conducted in user mode from a security perspective, kernel visibility is certainly critical to ensuring that a threat actor does not insert themselves into the kernel themselves and disable or remove the security products and features.

Ms. LEE. So is it your assessment then that it's not possible really and in realistic terms to do it outside of the kernel?

Mr. MEYERS. With the current kernel architecture, this is the most effective way to get the visibility and to prevent an adversary from tampering with security tools.

Ms. LEE. So it is the most effective way, but it is not the only way possible.

Mr. MEYERS. The—it is certainly the industry standard to use the kernel for visibility enforcement and anti-tamper and to ensure that you can stop a threat.

Ms. LEE. So you've testified thus far that you've made modifications to the phased rollout approach and also the predeployment testing. What other modifications has CrowdStrike made or changes to your internal practices to avert future similar incidents?

Mr. MEYERS. Sorry, I pushed the wrong button.

That is the primary changes that we've made. We've come up with an entire new mechanism by which we distribute the content updates. Again, making sure that customers have in their control the ability to select when they receive those updates is what will prevent that from happening.

Ms. LEE. Mr. Chairman, I yield back.

Mr. GARBARINO. The gentlelady yields back.

Without objection, the gentleman from Texas, Mr. Gonzales and the gentleman from South Carolina, Mr. Timmons are permitted to sit on the dais and ask questions of the witnesses.

I now recognize the gentleman from Texas, Mr. Luttrell, for 5 minutes of questions.

Mr. LUTTRELL. Thank you, Mr. Chairman.

Good morning—good afternoon, Mr. Meyers. Can you explain to me kind-of on a more granular level internal when internal testing, you said that there was a human element involved in this. I'm curious because you guys used the OODA loop method inside your company, correct? Big fan of it by the way, so great job. I'm just curious if we are doing internal testing in a way that most certainly would prevent this from happening and the human element is involved and it is not artificial intelligence that is pushing out this information. Can you walk me through that, please?

Mr. MEYERS. Absolutely. Thank you, Congressman, for the question.

The process for testing the content updates was reliant on validators.

Mr. LUTTRELL. How many? How many?

Mr. MEYERS. I have to get back to you on the exact number. But we tested each of the channels so each of the different rules that were inside that content file were tested individually. Those validators insured that the rules conformed and were compliant

with the very structure CrowdStrike had built for those content updates.

Mr. LUTTRELL. They test individually. There is something said about not testing them collectively. It seems like a very large—you guys touch a lot of things. You touch a lot of infrastructure in the United States, something that we count on you for, which you've been doing a great job.

You mentioned North Korea, China, and Iran. Our outside actors are trying to get us every day. We shot ourselves in the foot inside the house so I'm curious if we are testing these things individually, is there a point at which we test them collectively, before we push it out.

Mr. MEYERS. Yes, that's—thank you, sir. That's where we are now. So the new methodology is to test all of the content updates internally before they are to the early adopters.

Mr. LUTTRELL. So that's where the fault was, internal. We were testing the coding individually instead of collectively and one of them was off.

Mr. MEYERS. The testing process looked at each configuration and made sure that it conformed with the standard. It is now being tested internally before it's rolled out to customers and then the customers have control over when—what systems get those updates.

Mr. LUTTRELL. Yes, sir. I'm still trying to figure out exactly how this thing got launched with it not being absolute.

Mr. MEYERS. Thank you. The rules, the validator itself was in place for over a decade and we were released 10 to 12 of these updates every single day since we started using the configuration updates. That was tested against the standard to make sure that the configuration conformed with the standard are that CrowdStrike had a written for those configuration updates.

Mr. LUTTRELL. This happened to test positive and sent it out. I think I'm trying to find out did it test positive and we launched it or did it fail and we launched it accidently?

Mr. MEYERS. Thank you. Yes, it tested as clean or good and that's why it was allowed to roll out.

Mr. LUTTRELL. So as we unpack this, where exactly did it fail? This may be a complicated question to answer in a minute and 18 seconds.

Mr. MEYERS. I'll give it a try.

Mr. LUTTRELL. All right.

Mr. MEYERS. So content file triggered an issue within the kernel sensor. So that when the sensor process, the configuration it is almost like if you think about a chess board trying to move a chess piece to someplace where there is no square, that's effectively what happened inside the sensor. So when it tried to process the rule, it was not able to do what the rule was asking it to do, which triggered the issue within the sensor.

Mr. LUTTRELL. Should we have known that? Should CrowdStrike would know that about the kernel, correct or this was something that we weren't aware of?

Mr. MEYERS. This was kind-of a perfect storm of issues that resulted in the sensor failure.

Mr. LUTTRELL. OK. I'm going to need about 20 more seconds, Mr. Chairman. Are you good with that?

So knowing what we know now, what is the response mechanism in place, worst-case scenario this happens again for all the users?

Mr. MEYERS. Thank you. So this would trigger—this would be detected within CrowdStrike before it ever made it——

Mr. LUTTRELL. Because now we're doing it to code?

Mr. MEYERS. Yes.

Mr. LUTTRELL. Thank you, Mr. Chairman. I yield back.

Mr. GARBARINO. The gentleman yields back.

We are very lucky we were joined by our friend from New Jersey, Mr. Menendez.

Mr. SWALWELL. Very busy.

Mr. GARBARINO. Five minutes of questions, Mr. Menendez.

Mr. MENENDEZ. Mr. Chairman, Ranking Member, I don't often get to say what a privilege it is to serve not just with folks on this committee, but the two incredible leaders by the Chair and Ranking Member. I'm just so thankful for their friendship and stewardship of this subcommittee.

As we discuss today the global IT outage triggered by faulty CrowdStrike sensor update, disrupted critical services across various sectors. In my district passengers at New York Liberty International experienced delays and cancelations, some New Jersey hospitals had to delay or cancel procedures and some 9–1–1 dispatch centers were even rendered inoperable, jeopardizing public safety. This incident wasn't only a significant disruption but also preventable event that could and should have been avoided with basic quality assurance practices.

Our Government services rely and our constituents deserve the highest level of security and reliability. CrowdStrike must implement robust measures to prevent future incidences and ensure that their technology truly protects and serves our communities effectively.

A cybersecurity risk can continue to evolve. It is crucial that companies not only provide robust security solutions but also empower their customers to control and tailor their defenses in a way that best suits their needs. The root cause analysis also mentions increased customer control over rapid response content deployments. How does providing customers with control over rapid response content deployments improve overall security?

Mr. MEYERS. Thank you for the questions, Congressman.

Let me first start by saying again we apologize, we are deeply sorry for the impact for the folks at the airport and in the hospitals. We have a long legacy of stopping threats and that is our primary objective as a company.

In terms of how these controls will enable customers or constituents to have more control over what happens on their systems, it effectively gives them the ability to select which systems they can themselves test on and let's say that's the early adopters, they can select any number of systems that they would like to enroll in that early adopter program in order to receive those content updates before any of the other systems in their environment.

Then from there, they can have the rest of their systems on general availability. If there are systems that are particularly sensitive

and they want to withhold even for a few more iterations, they can do that. So this gives them complete control over where updates go and when they get them.

Mr. MENENDEZ. Thank you for that. I just want to make sure this all works right and there is the benefit of your customers, our constituents and so we're just trying to make sure we all get on the same page.

What type of support does CrowdStrike provide as the customer is making these individualized decisions to make sure that having a bespoke approach to adopting the sort-of new technologies, et cetera, that we believe that they are getting the full suite of options that they need for their particular industry, right? Because, you know, cybersecurity is obviously a quickly-evolving field and so we want to make sure that there are no gaps, right, for a particular customer or industry, now that they have a little bit more control over what they bring on-line on their systems.

Mr. MEYERS. Thank you, Congressman.

CrowdStrike I would say in my experience has been a customer-focused organization from the very beginning. Thirteen years ago when we launched the company in the wake of what was called the Operation Aurora where security tools of the day failed to detect Chinese adversaries who were conducting espionage operations against Western businesses. From the moment we launched the company we've been very focused on ensuring that we hear our customers and that we are here to support our customers, now we are a part of their mission whatever that may be.

We continuously hear from our customers through customer advisory boards. We are constantly engaging with customers. On the 19th of July we started round-the-clock phone calls talking to every customer that we could get ahold of in order to hear what was going on and them how we can help. We've also been briefing ISATs and Government agencies, whether it be CISA or others and working with Congressional staff in order to ensure that everybody's questions are answered. We do this throughout the year, not just in the wake of that incident.

So it's really, as I said earlier, a team sport. We need to work together with our customers, with the Government and with everybody involved to ensure that we are all marching in the right direction.

Mr. MENENDEZ. Yes, I appreciate that. Hopefully we will do a second round. I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentleman from Florida, Mr. Giminez, for 5 minutes of questions.

Mr. GIMENEZ. Thank you, Mr. Chairman.

I was gone for a little while so maybe you have answered this but did you say that CrowdStrike issues hundreds of updates daily?

Mr. MEYERS. Congressman, I had said that the 10 to 12 times per day we have issued content updates which contain the latest threat intelligence information to instrument our sensor, our tool, to understand what new threats are evolving. The threat landscape changes sometimes minute by minute. So in order to keep ahead of those threats to allow the CrowdStrike platform to detect and prevent those threats, it needs routine updates.

Mr. GIMENEZ. So 10, 12 times a day CrowdStrike will update its systems to react to a new threat that you've seen. Is that accurate?

Mr. MEYERS. That's accurate. I would say that it updates the configuration information, not the system itself.

Mr. GIMENEZ. The events of July 19, was that the system upgrade or what was that? It was something different than this 10 to 12 per day thing or what was it? Tell me what that was.

Mr. MEYERS. Thank you, Congressman. It is—that was a configuration update.

Mr. GIMENEZ. How often do you do that?

Mr. MEYERS. As I said, 10 to 12 times a day, sir.

Mr. GIMENEZ. So 10 to 12 times a day you got have these updates. You've done them every day, so you've done thousands of these updates. What made this one different? Do you run system tests on each 10 to 12 times a day you run a system test to make sure that this thing is not going to do more harm than good, I assume, right?

Mr. MEYERS. Thank you, sir. We—I will answer that question first, what caused this update is that the configuration update had a mismatch in fields that resulted in one of the fields not being linked to a rule. So you may have stepped out earlier, but I had said it was kind-of like on a chess board if the chess piece moved to a square that wasn't present then that would be an example of effectively what happened there. That——

Mr. GIMENEZ. So since you have gone through I don't want to go through it again. So do you this 10 to 12 times a day, you've done this thousands of times. This one moved the chess piece outside the board. Therefore, the computers didn't now how to figure wait a minute, that's outside the game. Therefore, I'm going to crash, all right. That's never happened before? You've never moved a piece outside the board?

Mr. MEYERS. This is the first time that this issue has manifested, to my knowledge.

Mr. GIMENEZ. Have you tried to move the piece outside the board, and was it caught some time before?

Mr. MEYERS. The validators that the configuration information went through was meant to ensure that it didn't move outside of the board.

Mr. GIMENEZ. So was the process—were your internal processes followed and then you just saw this is a problem with your internal process that you have to fix or was it somebody went outside of your processes?

Mr. MEYERS. Thank you, that's a great question. It was not a lack of following the process. This was a issue with the content validator. We've subsequently ensured that there's now additional steps in place so that this cannot happen again.

Mr. GIMENEZ. So it's your process, in your process.

All right. I'm going to switch gears and go to AI because I only have about a minute. AI, do you consider AI a threat to for cybersecurity?

Mr. MEYERS. That's a great question. AI I think can be——

Mr. GIMENEZ. I just ask great questions. I appreciate that.

Mr. MEYERS. It could be a threat or it could be a benefit. It could be used to facilitate and to ensure that cyber defenders have more

tools at their disposal that they could leverage AI to more quickly process information and analyze it.

Mr. GIMENEZ. So before I go, I only have 30 seconds I have to make a statement, so the nation that leads in AI would be better protected against a nation that's somewhat behind? The better your AI is, the better you're going to be at protecting yourself. The better you are at AI, I guess the better you are going to be at attacking your adversary. Is that correct?

Mr. MEYERS. I agree with your statement, sir.

Mr. GIMENEZ. Thank you. I have 8 seconds and hopefully you will have a second round. Thank you.

I yield back.

Mr. GARBARINO. I recognize myself for 5 minutes.

I want to get into it.

You called it the perfect storm happened, you know, fail safes failed, but can you talk about what was the perfect storm and why it will never happen again. You know, a lot of perfect storms and hundred-year floods are all happening now every other year.

I want to make sure that you all know what happened, can explain it, and then how you're making sure it's not going to happen again. We're dancing around it. I just—you know, let's get into the—let's get technical.

Mr. MEYERS. Thank you, Chairman. The content validator was looking at the content channel file, which had 21 fields in it. The content validator allowed those 21 fields to go out to the sensor fleet. The sensor was looking for a configuration rule that was not present. When it attempted to use that rule, that's where the sensor failed. So there was a—that's what caused the blue screen.

So that was detailed in RCA, and I don't want to—I don't know if I can explain it in the 3 minutes that are left here, but effectively, because the perfect storm was the content validator allowed the content configuration to go out to the sensor, and the sensor was not able to find the rule that it was looking for causing the issue.

Mr. GARBARINO. So you fixed it. It can't happen again.

Mr. MEYERS. It's a combination of process and the methodology at which we're now deploying those configurations. The configuration now is being treated as code whereas before it was treated purely as configuration information, so we're providing a lot more oversight and visibility into what that is and how it goes out to the system.

Mr. GARBARINO. How it goes out you all changed, but as the Chairman asked before, it's not all going out at once to everyone, so even if this does happen again, you've fixed it where it won't—it won't affect everyone all at once.

Mr. MEYERS. Yes.

Mr. GARBARINO. Another problem with fixing what happened, there was a—people had to be on-site, correct? You had to go to the different computers and reboot them individually. That's how you—that's how we got everything back up and running, correct?

Mr. MEYERS. Initially, the systems would need to be rebooted, the file deleted, and then the system allowed to boot from there. Subsequent to that, we came up with a USB boot disk that could be plugged in and the system could be rebooted and that would

automate the removal of the file, and then finally we were able to deploy an automated solution which allowed us to do this without manual intervention.

Mr. GARBARINO. OK. So there was reporting about CrowdStrike's faulty software update is largely focused on commercial operations, like emergency services, flights. But there was also big impact on Federal agencies, such as CFCC, Social Security, CBP, and even CISA. Although networks are becoming increasingly interconnected, Government networks should be isolated from commercial ones.

Why were Federal agencies impacted by this outage? Does your process for pushing out updates include—are there different updates to test for commercial versus Government business when you're dealing with your clients, or is it all the same? Is it one computer is it just one computer here?

Mr. MEYERS. The updates went to Microsoft Windows operating system sensors that CrowdStrike had deployed, so that would have impacted any system that was running Microsoft operating system with that particular version of CrowdStrike Falcon that was on-line during the time period that the channel file was distributed.

Mr. GARBARINO. As long as Microsoft was on that computer using that system, whether it was Government or commercial didn't matter. It was affected.

Mr. MEYERS. As long as the CrowdStrike sensor was running on the Microsoft operating system on the systems at that time, yes.

Mr. GARBARINO. OK. Wonderful. What—what did—you know what? I'm going to come back for my second round, because this is a much longer question than I have my time left for, so I'm going to yield back and then I'm going to recognize the gentleman from Texas, Mr. Gonzalez, for 5 minutes of questions.

Mr. GONZALEZ. Thank you, Chairman, and thank you, Mr. Meyers, for testifying before our committee. I tell you what, I was very not surprised, but disappointed to see how everything went down, but that's kind-of the way it works in this space. I was grateful on how quickly CrowdStrike responded when they did find an error. I'll tell you what, I mean, I'm in Government.

I don't hear people—I don't see people that fess up and said hey, we made a mistake, work to fix it, and then as you're doing that send a report out so other people don't fall in that same mistake. Usually it's try to cover it up and move on to the next thing, so I was grateful to the fact on how hard you all worked to get things back up.

I'm interested and I was grateful for the call that we got on literally days after it occurred. Clearly, you know your stuff inside and out. I'm interested in how do we make sure, you know, if this happens again that we're in a spot where we can fix it, right? I'd argue that CrowdStrike is probably one of the better organizations that are out there, so what if it's a different vendor that maybe doesn't have the same resources, the same integrity, and whatnot?

So I'm looking at it through the lens of, you know, speed is the name of the game in this industry, and a lot of times you want to get ahead of the problem before—as it's evolving. Your technical report, how—let's dive into that a little bit. I mean, how has that been received in the industry? How has that been received in Gov-

ernment? Have you had any conversations with CISA or others on the technical piece to what went wrong and how do we fix it?

Mr. MEYERS. Thank you for the question, sir. The—let me start by saying that we were immediately in contact with CISA and many of your staffs to talk about this issue when it happened. Once we had gotten most of the recovery under way, we issued a preliminary incident report, which is available on the website, which was effectively put out to ensure that everybody understood what we knew at that point in time.

We then gathered as many of our engineers as we needed to in order to start work on the comprehensive root cause analysis. We brought in external parties as well, and then we produced that root cause analysis as soon as it was available, which was, I believe, the first week in August or so. The dates are a little bit fuzzy at this point. But we had the RCA out.

The response that I've heard from most of the folks that I've spoken to have been that they appreciate the level of depth that that report went into, and I think more importantly, that the plan that we put in place to prevent this from happening in the future is something that everybody acknowledged to me was going to enable our customers to have more control.

Mr. GONZALEZ. One of the concerns I have is every company does it a little bit different. Like, there is no standardized process to it. That's just a little troublesome, because, you know, when everyone's doing it differently, you're relying on well, we've never had this problem before.

We're about to have a lot of problems that we've never had before and I want us to get ahead of it. I just don't want this to be a flash in the pan where, like, hey, you're in the flash today, someone else is in the flash tomorrow. Like, we're all in this thing together, and so I'm really focused on solutions, getting ahead of it.

Like I said, you know, 8 million people may have gotten impacted, but how fast you turned that around I thought was—I was grateful for that, but what happens when next time it isn't that fast? So my question is on—I'm trying to figure out what role Government plays in this.

So my question is I've introduced this piece of legislation that's called the National Digital Reserve Corps which would recruit cybersecurity professionals to help during major incidences that occur. Based on your experience with large-scale cyber incidents, do you think having a reserve of cybersecurity experts on stand-by would improve our response-and-recovery efforts?

Mr. MEYERS. Thank you for the question, Congressman, and I think that first I would say transparency is the answer to your initial question. It is important for CrowdStrike and for others to be transparent when these things occur, because every system is different, every product is different, they all have different components.

So they can't all be uniformly thought of so fixing one problem on one product isn't necessarily directly applicable to other products. That said, transparency is absolutely critical, and why we endeavored to be so transparent when this occurred.

As far as having additional reserve forces on stand-by, I think in a situation where there is a cyber threat, and again, this was not

an attack—cyber attack, I think that is certainly beneficial. There's never a situation where less skilled operators is going to be better.

Mr. GONZALEZ. I'm out of time. I appreciate you coming to testify before the committee, and once again, being transparent throughout this process, the good, the bad, and the ugly. With that I yield back, Chairman.

Mr. GARBARINO. Gentleman yields back. I now recognize the gentleman from South Carolina, Mr. Timmons, for 5 minutes of questions.

Mr. TIMMONS. Thank you, Mr. Chairman. I appreciate you letting me waive on this committee. I appreciate that your testimony regarding the changes that have been made to make sure this cannot happen again. For better or worse, the No. 1 reason it probably won't happen again is damages. I mean, it insures an estimated in excess of $5 billion in damages to your customers. I'm sure that there's going to be lawsuits and settlements for days.

Can we talk about making the victims whole? I mean, you know, whether it's airlines, other critical infrastructure, what steps is CrowdStrike taking to, I guess, make it right? Other than making sure it doesn't happen again, which is fantastic and your response has been very admirable, but how do we make sure that any other—any future incident is held accountable as it relates to making the victims of the breach whole? Wasn't it breach? Making victims of the incident whole. How does that work?

Mr. MEYERS. Thank you for that question, Congressman. We've been working with our customers to ensure that they are up and running. We've identified that as of 29 July, 99 percent of the sensors were back up and running and we're working with our customers to ensure that we are able to help them through any issues that they are dealing with and continuing to support them in any way that they need.

Mr. TIMMONS. I mean, tens of thousands, hundreds of thousands of people missed flights. Businesses were inoperable for days or weeks. I mean, again, this isn't necessarily about CrowdStrike. This is about future cybersecurity incidents and creating a system through which people can be made whole. So in addition to getting people back up and running when their systems were down, I mean, you all have insurance policies.

There's a wide variety of evil mechanisms that will create accountability. Are you able to speak to any of that, or is that something that your lawyers will probably tell you to not talk about?

Mr. MEYERS. Congressman, I know people who are impacted by this as well, and as I said earlier, we're deeply sorry for what happened. We are working with customers to ensure that they have everything that they need to get back on-line. Most of them are on back on-line and ensured that they have what they need to feel comfortable that they're working with CrowdStrike. We're continuing to rebuild that trust. Trust takes years to make and seconds to break, and we understand that we broke that trust and that we need to work to earn it back.

Mr. TIMMONS. Do you think your customers care that this was an innocuous fat finger as opposed to an actual breach? I mean, there's still damages associated with both, so I mean, again, going forward, the global economy needs to have consequences for all

types of cybersecurity shortcomings, so I mean, do you distinguish between a breach and this faulty update?

Mr. MEYERS. Yes. I would say that there is a difference between a breach and when——

Mr. TIMMONS. One that I can tell my constituents that missed flights and were stuck in airports for weeks that they'll care about? Probably not. Again, you don't want to talk about the damages and making victims whole, but I think that's an important part of this. You're taking additional steps, which are very important to make sure that it doesn't happen again, but at the end of the day, part of this is making it right with the people that missed flights, that weren't able to engage in commerce, and that's part of the conversation that we need to be having, because that is the deterrent threat to the future and future incidents will occur.

The reason that businesses that have major cybersecurity breaches end up settling for hundreds of millions and billions of dollars in certain circumstances is because that is how they are made whole. Again, this was a fat finger, so it's not the same as a breach. I get what you're saying. But the damages are still the same in many respects. So we're going to, I'm sure, hear more about the manner in which the—your customers and their customers were made whole as a result of this incident, and I think that that's an important part of the story, because ultimately, that's the accountability that our system provides to make sure it doesn't happen again, the deterrent threat.

With that, Mr. Chairman, I yield back. Thank you.

Mr. GARBARINO. Gentleman yields back. Thank you for joining us today. We're going to start our second round of questioning. I'm going to start by first recognizing the gentleman from Florida, Mr. Gimenez, for 5 minutes of questions if he has them.

Mr. GIMENEZ. Thank you, Mr. Chairman, and I want to kind-of continue on what I ended up with, which was with AI and the problems that AI—does AI pose a threat right now and what do you see as the threat from AI in the future? If you can elaborate on that.

Mr. MEYERS. Absolutely. Thank you, Congressman. The threats from AI that I see today are primarily—and what we've seen adversaries using various AI for, whether it be large language models or stable diffusion or different algorithms that can be used to generate new content has been primarily around disinformation, misinformation, and enabling faster research. In other words, threat actors have used artificial intelligence OOMs to automate writing scripts while—that they can use during an intrusion or during a ransomware operation.

Mr. GIMENEZ. If I can interrupt, will that mature into AI writing code that will be malicious in nature?

Mr. MEYERS. We've—I've personally done some research in that area, and I think right now it's not there. You still need to be very familiar with the tool chain and you need to be able to actually compile the code and debug it and understand where there's issues, but every day this technology gets better and it's something that we need to keep a close eye on to ensure that we understand how threat actors may use it as well as good actors.

Mr. GIMENEZ. Yes. I mean, AI scares me and that's why we have to be on top. Because the only defense against AI in the future, I mean, if it gets totally mature and it just starts writing code, and you have to have AI on your side that writes the counter code just as fast as it's getting this code. So you're going to have this—you're going to have millions of attacks per day and you have to defend against millions of attacks per day because these things will just generate attack after attack after attack. Now, then you put that with quantum computing, now you really got a problem.

So where is your company on that? I mean, you're a leader in cybersecurity. I'm concerned about the fact that something—a program that was supposed to protect systems against cyber attacks actually kind-of destroyed the system they were trying to protect. Didn't destroy it, but certainly disrupted it. All right? So in the future, I can see this as being a tremendous problem and a tremendous risk. It may be that the future says that we're going to have to—we can't be so connected anymore because of the vulnerabilities involved. Can you foresee such a future?

Mr. MEYERS. I don't foresee a future where things get—need to be disconnected necessarily, but I think that we need to be very careful and thoughtful as we roll out artificial intelligence solutions. Happy to work with your staff and yourself to spend more time on that issue if you'd like.

Mr. GIMENEZ. Well, I don't think it would be in your best interest for us to disconnect. All right? But I'm not sure that it wouldn't be in our best interest sometime in the future for security reasons to disconnect somewhat, that somehow, no matter what comes in, that the system won't be disrupted. Yes, that's a hiccup or I just got punched in the face, but I'm not going to get knocked out. All right?

That's the problem that we have. My fear is that an adversary, before they launch something, won't try to knock us out, and I think we're vulnerable to that right now, that we can get knocked out. Our electrical systems can get knocked out, transportation systems can get knocked out all at the same time causing massive disruptions. I don't think anybody can tell me no, that's not possible. It is possible, right?

Mr. MEYERS. What I would suggest, sir, is that I think in the future we can see that organizations will have their own AI workloads. They'll be deploying artificial intelligence to solve customer challenges, business challenges, and it won't be a handful of AIs that are being used across the globe. I think we'll see very localized artificial intelligence workloads, and this is something that we need to be thinking about, how do we secure those AI workloads into the future, because adversaries can leverage that AI workload. They can poison the data that goes into AI training. So there's a whole new wave of horizon threats that pertain to AI and something that I think is a very critical thing for us to be talking about.

Mr. GIMENEZ. Thank you. My time is up. I yield back.

Mr. GARBARINO. Gentleman yields back. I recognize the gentleman from Texas for a second 5 minutes, Mr. Gonzalez.

Mr. GONZALEZ. Thank you, Chairman, and thank you again for allowing me to speak today. Mr. Meyers, I just would highlight there are very few people in Congress that really understand this

issue, and this is one of the committees—I mean, you have a Chairman, you have Members on this committee that are—that want to find solutions, that want to get ahead, as Mr. Gimenez just mentioned.

You know, the future is already here, and I worry what role Government is going to play. I would just once again highlight to you, like, this isn't just a one-off. The more that your team and your—you all can be working with our staff as we build out a meaningful responses either through the appropriations process or through legislation, I think it's very critical, because I do worry that we'll get it wrong, right? Or we'll be delayed in it or it will have meaningful intentions, but have second- and third-order impacts that may make it more difficult for you whether it's a self-inflicted kind of incident or whether it's an intrusion. So I just would highlight, you know, once again, thank you for coming and testifying but, you know, let's work toward fixing this long-term on other issues that happen.

The other—so the question I have for you is from an industry standpoint, is it more impactful that Government get out of your way? I'm trying to frame it the right way, you know, without putting you on the spot, because I want to get as real an answer as possible. Maybe I'll frame it this way. In your dealing with CISA as you went through this intrusion, or as you went through this incident, I'm sure you probably dealt with them far more than you had in the past. What was a takeaway that, you know, that you think that we can improve on from a Government response, Government interacting with industry on dealing with a real-world situation to get things back on track? What was one of your takeaways that maybe this committee could work on?

Mr. MEYERS. Thank you, Congressman. First let me say it's an honor to be here. Thank you for having me. We work with CISA on a daily basis. We've been a—we're a plain cooler at JCDC and have been working hand-in-hand across the U.S. Government as well as other family governments every single day, and the way that we succeed in my mind is through public and private partnership. We need to all be able to share and work off the same sheet of music.

We track over 250 threat actors today that are coming from places like Iran, Russia, North Korea, but other countries that haven't made it into the press so to speak, and a whole bevy of threat actors that are engaged in ransomware and data extortion operations as well as hactivists who are looking to conduct hack-and-leak operations.

So I guess the one takeaway I would say is that in this situation, our job was to inform the Government and inform your staff about what was going on within CrowdStrike being transparent so that they could know that this, No. 1, wasn't a cyber attack, and No. 2, what the impact was what we're doing to remediate that.

I think in the situation where there is a cyber incident, then the responsibilities change and it becomes us supporting the Government, helping to understand who these threat actors are, what they're after, and how to stop them. So it depends on the situation, but I would reiterate that private-public partnership is absolutely

essential, because this is a team sport and we all are on the same team.

Mr. GONZALEZ. Appreciate the response. I would just close with this. This is the committee you want to work with, because guess what? There is where legislation is going to come out of that's either going to make your job easier or harder, right?

The intentions are going to be there. Best intentions for our country and our allies to defend against these adversaries, some of which you mentioned that are trying to kill us every single day, so that's what we're up against and we need partners, and I want to make sure from a legislative standpoint we're getting it right. We're committed on our side, but we need partners, right? Not everybody up here has the same level of expertise.

You try—I mean, I read that—I read the outage report right before I went to bed for a reason, right? I mean, it's very technical, right? So once again, thank you for coming and testifying. You're a brave man. Please continue to work with the committee as we find solutions. Thank you. I yield back.

Mr. GARBARINO. Gentleman yields back. I now recognize myself for 5 minutes of questions. Mr. Meyers, other cybersecurity providers, competitors of yours have said that the access to the kernel, so much, how many updates you're pushing out daily is—goes against industry standards and is not safe. What would you say in response to that?

Mr. MEYERS. I'm not aware of any industry standards that govern how or what to do with regards to any one operating system or best practice with that regard. I can tell you that when we launched CrowdStrike 13 years ago, we did so with the mission to stop bad things from happening to good people, and we've worked tirelessly in the last 13 years to ensure that our products, our services, and our intelligence information is the best possible product that our customers can consume.

I would say that we got it wrong in this case and we are running from what happened and we've implemented changes to ensure that that doesn't happen again.

Mr. GARBARINO. I understand that, and would you think now, because I believe you testified before you do maybe a dozen a day updates, because that's what you do. You find the threat and you update the system to protect against that threat. You think it's—you will still continue to do 12 a day, or as many as needed, or will this—will you be more—I don't even know if conservative is the right word, but more conservative in your approach on how many updates you will have daily?

Mr. MEYERS. We will continue to update our product with threat information as frequently as we need to in order to stay ahead of the threats that we're facing.

Mr. GARBARINO. In your belief, that is access to the kernel as much as you have it and updates as much as you have it as needed for cyber—for your clients' cybersecurity?

Mr. MEYERS. I think as we said earlier, speed does matter in this domain in order to stay ahead of these threat actors, and the visibility that we get through the kernel, the performance that you gain through using the kernel, the ability to stop bad things, the

enforcement mechanism that's provided through that kernel, and the anti-tamper to stop a threat actor——

One of the threat actors that we track very closely is a group called Scattered Spider who has been using techniques to elevate their privilege into the kernel in order to disable security tools on a regular basis. In order to stop that from happening, we will continue to leverage the architecture of the operating systems that we're on in the most effective way that we can to stop those threats.

Mr. GARBARINO. Is it just unlucky that this update was for a Microsoft operating system? Could this have happened to any—pretty much any other operating system, right? It could have been on the update. It was just an unlucky coincidence that it was Microsoft?

Mr. MEYERS. I would say that a lot of businesses rely on Microsoft for their operating systems, and I think that's where the number of impacted systems from this update came from.

Mr. GARBARINO. But, I mean, the problem was with the update. It wasn't with Microsoft system. It was with the update was faulty.

Mr. MEYERS. This was a CrowdStrike issue.

Mr. GARBARINO. Are you developing any—I want to make sure I got this in. Are you developing any agentless technologies to scan for infrastructure remotely which could avoid this type of outage in the future?

Mr. MEYERS. I'm sorry, can you repeat that?

Mr. GARBARINO. Are you developing any—are you developing agentless technologies to scan infrastructure remotely which could avoid this type of outage in the future?

Mr. MEYERS. Thank you. We have a number of platforms that we provide to our customers, including attack surface management tools which can scan without an agent or a sensor in place, but in order to detect and to prevent threats, you need to have that enforcement mechanism in place on the operating system in order to stop that from occurring.

Mr. GARBARINO. OK. This last thing, because I'm going to yield back in a second and let Mr. Swalwell go. Is there now something in place, because what happened—someone didn't catch it. There was an additional parameter in the channel file before it was—went through content interpreter or the validator. Is there now a process—is there something new in place to prevent that from happening again?

Mr. MEYERS. Yes, sir.

Mr. GARBARINO. OK. Thank you. Gentleman from California is recognized for his second round of questions, 5 minutes.

Mr. SWALWELL. Thank you. I wanted to follow up on the line of questioning that Ms. Lee and I were kind-of going back and forth with with regard to the kernel. Part of the discussion at the Microsoft Endpoint Security Summit involved reducing reliance on the kernel. My understanding is that Microsoft agreed at the summit to make additional capabilities available at the user level. Do you know the time line for that process and do you have a sense of how Microsoft and security vendors will engage to reduce the kernel and more additional activity, you know, to the user space? How

would you reduce risk to the kernel and move it to the user space I guess is the question?

Mr. MEYERS. Thank you. The—I don't have that time line available. Happy to follow up with you on that. What I will say is that things can crash in user space too, and so this is not unique to the kernel space.

Mr. SWALWELL. Trade one set of risks for another, right?

Mr. MEYERS. There's definitely things that can break in user space as well as in the kernel space, yes, sir.

Mr. SWALWELL. The relevant update in this incident only affected, as you've pointed, out Window systems, but my understanding is that Apple's restrictions on kernel access might have prevented a similar incident from taking place on Mac systems.

Do you view Apple's restrictions on kernel access to be beneficial or do they negatively impact the effectiveness of security software like yours?

Mr. MEYERS. We have security products that work on Windows systems, Apple systems, and Linux systems as well. We leverage all of the features of those various operating systems. They have pros and cons for each and we leverage everything in order to have the most effective security solution for those platforms.

The Windows architecture is an open architecture as I mentioned earlier. Apple has a tighter supply chain, and with Linux you have to precompile the kernel for every possible configuration of hardware that you would want to support, so there's different features of each kernel.

Mr. SWALWELL. Would you agree, though, that if something crashes in the app space, it's limited in its effect to the app, whereas if something crashes with the kernel and Microsoft, it could crash the whole system?

Mr. MEYERS. Yes.

Mr. SWALWELL. I've got about 2½ minutes left. Is there anything that we didn't cover that you think would be helpful for us to understand? Anything that you want to just revisit and further articulate?

Mr. MEYERS. I think it's important to note that this is not a cyber attack. This is something that happened within the system during an update process which we've spent a considerable amount of thought and effort to ensure that this doesn't happen again.

My concern is, if I may, the cyber threat actors that we're seeing across the globe, this is something that we need to be paying close attention to. We're seeing the constant evolution of those threat actors looking to subvert systems. They've moved into the identity space stealing user names and passwords and are leveraging identity access to move into new environments and to conduct additional ransomware and data extortion attacks, so this is an area that continued—would like to continue working with the committee on and anything that we can do to help.

Mr. SWALWELL. Great. Mr. Chairman, do you have anything you wanted to ask?

Mr. GARBARINO. No. I'm just saying—just speed, with the cybersecurity—we don't work with speed here in Congress unfortunately.

Mr. SWALWELL. Speed, what's that? We don't recognize that. I yield back.

Mr. GARBARINO. Gentleman yields back. I want to thank the witness for his valuable testimony and the Members for their questions. I think this was a very good hearing. The Members of this subcommittee may have some additional questions for you and we would ask that you respond to these in writing. Pursuant to committee rule VII(D), the hearing record will be held open for 10 days. Without objection, the subcommittee stands adjourned.

[Whereupon, at 4:04 p.m., the subcommittee was adjourned.]

APPENDIX I

QUESTIONS FROM CHAIRMAN MARK E. GREEN, MD FOR ADAM MEYERS

Question 1a. According to an article in Semafor dated September 12, almost 2 dozen former CrowdStrike employees claim that the company prioritizes speed over quality.

Would CrowdStrike attribute the global IT outage to a lack of quality control?

Answer. No. CrowdStrike maintains rigorous testing and validation throughout its entire software development and configuration information creation processes. As part of these testing and validation processes, CrowdStrike's software code is certified by Microsoft through the Windows Hardware Quality Labs (WHQL) program and tested through a quality assurance process. Configurations read by the code are validated to conform with the expected input specification. While code is updated less frequently, new configurations are sent with rapid occurrence to protect against threats as they evolve.

On July 19, 2024, using a long-standing, routine process, we updated threat detection configuration information leveraged by the sensor, without needing to update the sensor's code. These new threat detection configurations were validated through regular validation procedures as correct and sent to sensors running on Microsoft Windows devices. As we describe in detail in our Technical Root Cause Analysis, the July 19 incident stemmed from a confluence of factors that ultimately resulted in the Falcon sensor attempting to follow a threat detection configuration for which there was no corresponding definition of what to do.

Question 1b. Does CrowdStrike believe that employees experience "rushed deadlines, excessive workloads, and increasing technical problems?" Why or why not?

Answer. No. CrowdStrike's mission is to protect good people from bad actors. Our employees are committed to this mission and work hard to protect against rapidly emerging threats. CrowdStrike has grown its headcount consistently year over year, including in research and development. CrowdStrike has been recognized as one of the Fortune 100 Best Companies to Work For for the last 4 years.

Question 1c. How many complaints from employees has CrowdStrike received about issues related to quality control in the last year?

Answer. CrowdStrike receives, evaluates, and incorporates a range of feedback from its team. CrowdStrike is committed to ensuring the resiliency of our products through rigorous testing and quality control.

Question 1d. How does CrowdStrike handle internal feedback or complaints from employees, particularly regarding those related to lack of quality control?

Answer. As noted above, CrowdStrike receives, evaluates, and incorporates a range of feedback from its team. We are committed to safely and responsibly developing our products with the care they require to be effective. While CrowdStrike is actively reviewing its quality process, we have also engaged 2 independent third-party software security vendors to conduct further review of the Falcon sensor code for both security and quality assurance.

Question 2. How much does CrowdStrike rely on AI or automation to update its products versus manual decision making? Please be specific about where and how you use AI or automation in its software update process.

Answer. The July 19 incident was not caused by AI.

Question 3a. CrowdStrike's Root Cause Analysis (RCA) states "The new IPC Template Type defined 21 input parameter fields but the integration code that invoked the Content Interpreter with Channel File 291's Template Instances supplied only 20 input values to match against. This parameter count mismatch evaded multiple layers of build validation and testing. . . .".

Please explain why no one caught the additional parameter in the channel file before putting it through CrowdStrike's Content Interpreter or Content Validator, which the RCA said resulted in a mismatch.

Answer. As we describe in detail in our Technical Root Cause Analysis, the July 19 incident stemmed from a confluence of factors that ultimately resulted in the Falcon sensor attempting to follow a threat detection configuration for which there was no corresponding definition of what to do. (See answer 1.a for further details.)

Question 3b. Since the July 19 outage, has CrowdStrike created a specific test for "non-wildcard matching criteria in the 21st field," which the RCA said was lacking and contributed to the system crash?

Answer. CrowdStrike took the following mitigation actions, as described in the Technical Root Cause Analysis: "Bounds checking was added to the Content Interpreter function that retrieves input strings on July 25, 2024. An additional check that the size of the input array matches the number of inputs expected by the Rapid Response Content was added at the same time.

"These fixes are being backported to all Windows sensor versions 7.11 and above through a sensor software hotfix release. This release will be generally available by August 9, 2024.

"The added bounds check prevents the Content Interpreter from performing an out-of-bounds access of the input array and crashing the system. The additional check adds an extra layer of runtime validation that the size of the input array matches the number of inputs expected by the Rapid Response Content" (Pages 3–4).

These mitigations, referenced in the RCA, have been implemented.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR ADAM MEYERS

Question 1. Does CrowdStrike's framework for disaster recovery plans align with industry standards, such as the National Institute for Standards and Technology or the International Organization for Standardization? If yes, how often does CrowdStrike audit its plans to ensure they are ready and compliant?

Answer. CrowdStrike's security and recovery practices are designed to align with widely-accepted industry standards and best practices, including those outlined by the National Institute for Standards and Technology and the International Organization for Standardization. CrowdStrike reviews its business continuity controls and disaster recovery plans at regular intervals.

Question 2a. Did CrowdStrike analyze the security impact of any proposed changes prior to implementation in its FedRAMP environments, consistent with documented NIST security controls? Please explain.

Question 2b. What steps will CrowdStrike take to ensure Federal systems are not impacted if an outage of this scale happens again?

Answer. We value our Federal customers, and appreciate the partnerships we have with them. The new controls we implemented following 19 July account for customer needs across our entire user base, including U.S. Federal agencies and those operating within CrowdStrike FedRAMP environments. We have implemented a staged deployment strategy for content updates, which will enhance resilience across the full customer base. We also have engaged third-party vendors to conduct further review of the situation, provided our customers more control over the updates they receive, and prevented the creation of the problematic type of file at issue here.

Question 3. CrowdStrike's Root Cause Analysis (RCA) of the July 19th outage notes that in February 2024, CrowdStrike released a new sensor version that "developed and tested according to our standard Sensor Content development processes and was integrated into the sensor to prepare for utilization in the field."

Please expand upon this claim and explain why new testing processes were not implemented for a new sensor version.

Answer. Sensor version 7.11 was subject to both routine and new tests prior to being made generally available to customers on February 28, 2024.

Question 4a. How does CrowdStrike think this outage will impact the cybersecurity industry more broadly?

Will cybersecurity vendors be more conservative in rolling out updates?

Answer. We will continue to update our product as frequently as is necessary to empower our customers to stay ahead of rapidly-evolving threats. As noted above, customers also now have greater control over updates, including timing.

Question 4b. How is CrowdStrike working with cybersecurity partners to ensure changes to kernel access are implemented securely and prioritize resilience?

Answer. Cybersecurity solutions designed to protect the Microsoft Windows operating system require kernel access for performance, anti-tampering, visibility, and enforcement. CrowdStrike participates in official cybersecurity software initiatives, including those related to the development of software for Microsoft Windows. Following the incident, CrowdStrike engaged in a technical summit focused on sharing

best practices related to Microsoft Windows kernel-level software development enhancements. CrowdStrike looks forward to the opportunity to continue to work with ecosystem partners for safe, comprehensive, performant, and reliable processing of security-related data.