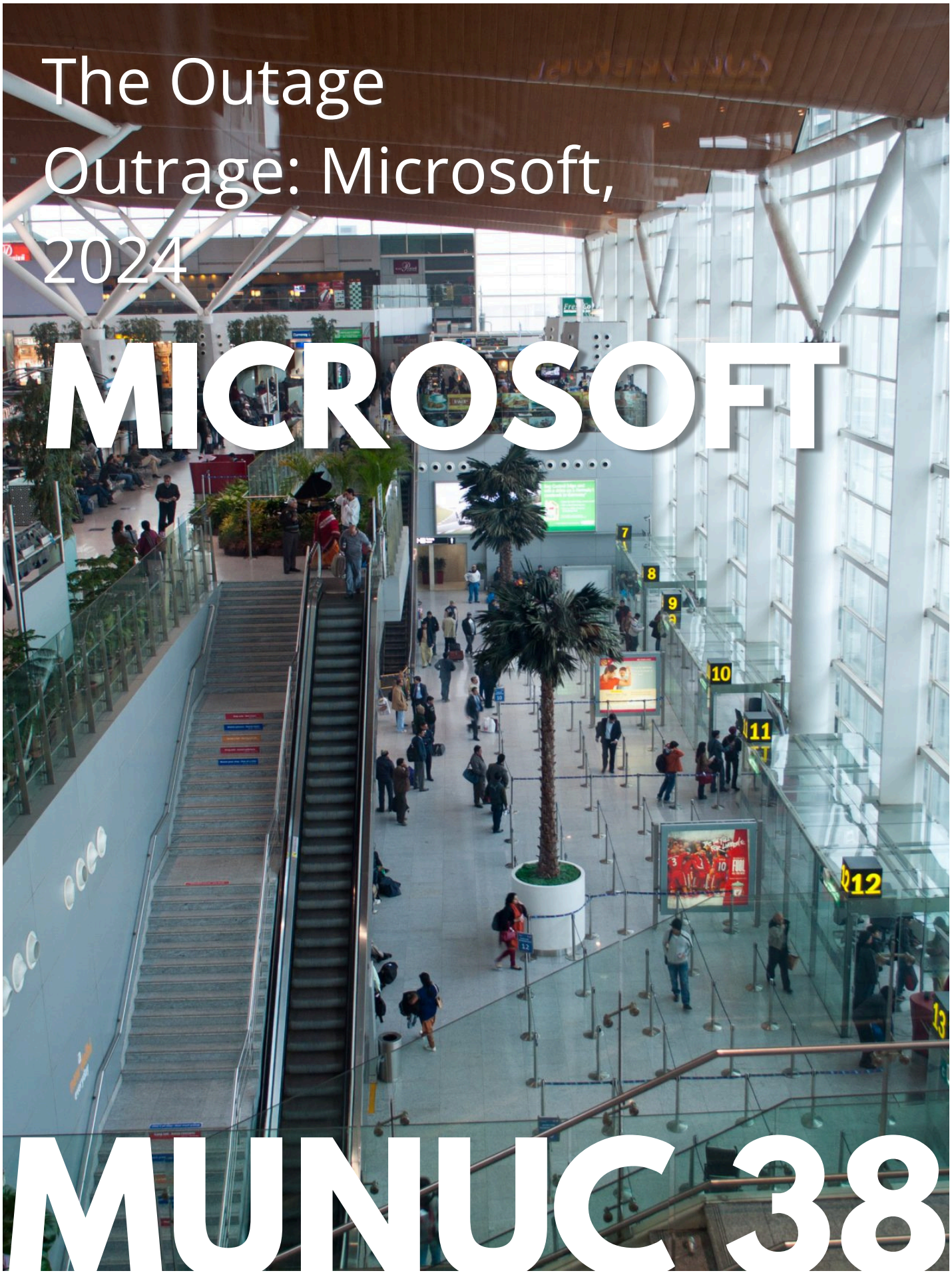
The Outage Outrage: Microsoft, 2024



MUNUC 38

Model United Nations of the University of Chicago

Chair Letter

Hello everyone,

I'm Sameer, and I am excited to serve as your chair for *The Outage Outrage: Microsoft 2024*. I'm a sophomore at the College majoring in Economics (with a specialization in Business Economics), originally from the great city of Lahore in the country of Pakistan, though I am currently navigating the urban storm of Chicago! I was an avid golfer back home, but for now I'll settle for chairing digital disasters instead of hitting birdies.

This committee offers an exciting and urgent opportunity to engage with one of the defining questions of our time: what happens when the very backbone of the digital world collapses? You'll be stepping into a room of global powerbrokers, scrambling to restore stability while navigating blame, politics, and the fundamental question of trust in a hyperconnected age.

Given the dynamic nature of this crisis, I expect delegates to come prepared not only with background knowledge, but with flexibility, creativity, and a collaborative spirit. You will need to think on your feet as new information emerges, negotiate alliances across corporate and governmental lines, and craft actionable directives that can shape the world's response. Success here lies not in isolated speeches, but in your ability to work with the people sitting beside you to build real solutions—and manage the inevitable political fallout.

For me personally, this committee also resonates deeply. Having grown up in Pakistan—a country where questions of digital sovereignty, infrastructure fragility, and public-private dynamics are front and center—I find it fascinating to explore how global systems function (or fail) when pushed to the brink. I encourage you to approach this simulation not just as an

exercise in crisis management, but as a broader exploration of what trust, accountability, and resilience mean in today's digital world.

As always, the CDs, and I are here to support your preparation and success. Please don't hesitate to reach out with any questions about the structure or content of the committee. I look forward to seeing you all in the eye of the storm—and to witnessing how you navigate it.

Best of luck, and see you soon.

Mohammad Sameer Nasir

Chair, The Outage Outrage: Microsoft 2024

msnasir@uchicago.edu

Crisis Director Letters

Hello delegates!

My name is Annika Naramreddy, and I am thrilled to be one of your Crisis Directors for *The Outage Outrage: Microsoft 2024*. A little bit about myself: I was born in sunny San Jose but moved to Hyderabad when I was 4 and relocated again to Dallas two years ago (so when someone asks me where I'm from, my answer is "it's complicated"). Currently pursuing Data Science and Economics at the University of Chicago, with aspirations of attending law school, I am particularly intrigued by the intersection of AI and machine learning with the legal domain, especially in environmental law. Outside of my academic and career interests, I love exploring the Chicago food scene, reading, and am always down to take a walk to nowhere.

I've been actively involved in MUN since 5th grade and in both UChicago's college conferences as well. This past year, I served as Crisis Director for *The Court of the Nizams: Hyderabad 1947*. I've also previously been an Assistant Chair for *JCC Bakumatsu Japan, 1860: The Bakuhan Government* at MUNUC 36 and for *On the Chopping Bloc: Food Policy in a Boiling World* at ChoMUN XXVII. My passion for MUN has only deepened over the years, serving as a catalyst for personal growth and meaningful connections. It's with great enthusiasm that I take on the role of Crisis Director at MUNUC 38, hoping to facilitate an enriching experience for all participants.

As someone fascinated by technology and its societal impact, I'm especially excited to see how you approach the chaos of a corporate crisis in *The Outage Outrage: Microsoft 2024*. From navigating aviation nightmares to managing supply chain meltdowns, this committee offers

endless room for creativity, strategy, and bold decision-making. I can't wait to see the directives, alliances, and unexpected plot twists you bring to the table as we unravel this modern tech crisis together.

In case you have any questions or want any insider insights into the city, feel free to reach out to me at anaramreddy@uchicago.edu. Looking forward to seeing you soon!

Best,

Annika Naramreddy

Crisis Director, The Outage Outrage: Microsoft 2024

anaramreddy@uchicago.edu

Hello delegates!

My name is Arzoo Usgaonkar, and I'm thrilled to serve as one of your Crisis Directors for The Outage Outrage: Microsoft 2024. A bit about me: I'm an international student from Mumbai, India, currently pursuing a BA in Economics and Psychology and an MA in Psychology at the University of Chicago. My academic interests center around understanding human decision-making, particularly the cognitive biases that often steer us off course. I hope to help people better recognize these lapses in our cognition—and ultimately make wiser decisions for themselves, their communities, and the planet. Outside the classroom, I spend a good amount of my time reading, exploring Chicago with my friends, baking, and occasionally doing some kind of arts and crafts (I've been really intrigued by pottery).

My Model UN journey began in 7th grade, and I've had the chance to participate in UChicago's MUN world through both MUNUC and ChoMUN. At MUNUC 37, I chaired *The Court of the Nizams: Hyderabad 1947*, and at ChoMUN XXVII, I chaired *On the Chopping Bloc: Food Policy in a Boiling World*. Previously, I served as an Experienced Assistant Chair for *JCC: Bakumatsu Japan, 1860* at MUNUC 36, and as an Assistant Chair for *The Maratha Confederacy* at ChoMUN XXVI. MUN has shaped me in countless ways: it's boosted my confidence, sharpened my public speaking skills, and introduced me to some of my closest friends. That's why I'm so excited to help bring this conference to life for you.

The Microsoft outage we'll be exploring was a crisis of massive proportions with far-reaching consequences. It underscored just how vulnerable we are to disruptions in digital infrastructure and raised urgent questions about our dependence on a handful of tech giants for internet security. Throughout this committee, I hope to see you, delegates, develop dynamic character arcs and approach this challenge with creativity, thoughtfulness, and resolve.

If you have any questions—or just want a great restaurant recommendation—feel free to reach out to me at arzoo@uchicago.edu. I can't wait to meet you all soon!

Best,

Arzoo Usgaonkar

Crisis Director: The Outage Outrage: Microsoft 2024

arzoo@uchicago.edu

Sensitivity Statement

The 2024 Microsoft outage represents one of the most severe global digital failures in recent memory, triggering cascading disruptions in healthcare, aviation, banking, governance, and communication systems around the world. Our crisis simulation imagines the world at the moment of that collapse—a world where access to information, safety systems, and critical services vanished in an instant.

In light of this, we ask all delegates to approach this committee with empathy, care, and 21st-century values. You may be representing a country or a corporation, but you must always reflect respect, equity, and human dignity. This applies to your private notes, directives, speeches, unmoderated caucuses, and even your conduct outside of committee time. Discriminatory, insensitive or dehumanizing behavior (including sexism, racism, homophobia, religious discrimination, or any other form), whether in character or not, will not be tolerated under any circumstances.

We take ensuring the comfort and respect of every individual at MUNUC extremely seriously, and we will take action against delegates who do not display the same. Please keep this in mind as you craft your arcs. We look forward to having you in committee!

Structure and Mechanics

The Outage Outrage: Microsoft 2024 is a Hybrid Committee. This means you'll experience two styles of debate during the conference: crisis sessions and general assembly (GA) sessions. That may sound a little intimidating at first, but once you know how it works, you'll know it's the best of both worlds.

This section of the background guide explains how the committee works so you're ready to go from day one. We recommend reading it twice to get comfortable with the flow!

Part 1: Crisis Sessions

Our committee will meet for five sessions in total over the course of the conference. The first three will be crisis sessions.

What is crisis? Think of it as responding in real time to problems that result from the committee's agenda. In our case, Microsoft's systems have just crashed—as delegates (representing both countries and Microsoft leadership), you'll be tackling the fallout as it unfolds. You will not know what crises are coming beforehand. Those that occurred in 2024 and those in our background guide are just for you to get an idea of the kinds of problems that arose. Expect surprises from us!

Here are some key elements of crisis sessions to help you understand how they work:

1 | Crisis Breaks

About every 30 minutes, our Assistant Chairs (ACs) will enter the committee and perform a short skit. These roleplays bring new problems caused by the outage. Each crisis break sets the direction of debate until the next one.

2 | Role of Delegates (Mods & Unmods)

After each crisis break, the committee will function through a combination of Moderated and Unmoderated Caucuses.

A. Moderated Caucus (Mods): These are usually right after a crisis break. Delegates make short speeches. For example, if a "Motion for a 5/30 moderated caucus on the crisis at hand" is raised, this means that the total time will be 5 minutes, and each delegate will make a 30 second speech. Some quick math tells us that 10 delegates will make speeches, and the topic they'll speak on is "the crisis at hand."

B. Unmoderated Caucus (Unmods): Up to 8 minutes long for our committee. Delegates move around, form blocs (groups), and discuss informally to craft quick solutions to the current crisis. Once those solutions get on paper, they become directives.

3 | Directives

These short-term solutions are written like Model UN clauses. Directives are typically drafted in groups during Unmods and submitted to the Chair. The Chair will read them in order of submission. One delegate may speak for, and one against, before a vote. If a directive passes, its proposal takes effect in the "real world." The clauses affect the crisis as it unfolds, so write carefully!

4 | Notes & Backroom

The backroom is one of the most exciting parts of the crisis. While debate continues in the room, you can also send notes to fictional characters outside the committee. At the start, you'll receive two notepads. Write to anyone you like to gather information, build resources, or attempt actions that influence the committee; our Assistant Chairs will respond to you in character. Over time, some of your actions may directly shape the course of the crisis and be part of our crisis breaks.

For some direction, we expect your notes in session one to focus on building resources, while those in sessions two and three will be directed towards implementing various things. (Pro tip: read your character bio carefully, it has valuable hints about your character that can help shape your arc!)

Some guidelines for our notes are:

1. No note should exceed one page.
2. Please add a TL;DR (2–3 bullet summary) at the bottom, which summarizes your asks.
3. Keep notes appropriate and legible.

Part 2: General Assembly Sessions

The final two sessions will look more like a traditional Model UN committee. You'll no longer have notes or the backroom. Instead, the committee will focus on longer Mods and Unmods, during which you'll form blocs and draft working papers. Working papers combine multiple directive-like clauses into one document. These are debated, refined into draft resolutions, and then voted on.

Your goal in GA will be to create a charter or roadmap to strengthen digital infrastructure and prevent similar crises in the future. Think long-term solutions, in the spirit of the UN.

Feel free to check out the MUNUC website's Prep and Resources Section if you would like more guidance! The Traditional Committee, Hybrid Committee, and Crisis Committee trainings all have helpful content that will help this section make more sense. If there's anything you have doubts about or would like clarification on, as always, feel free to reach out (our emails are in our Chair & CD Letters at the top of this background guide). *Please email all three of us, so that one of us can get back to you as soon as possible.*

Context of the Problem

In the early decades of the 21st century, the world underwent a transformation arguably as profound as the Industrial Revolution: nearly every facet of human life became intertwined with a vast, invisible network of digital systems. From the pulse monitors in hospitals to the algorithmic trades in stock exchanges, from air traffic control towers in Chicago to water supply systems in Karachi, everything now rests on lines of code.

This digital network promised unimaginable efficiencies and breakthroughs. However, it also led to something far more precarious: an unprecedented global dependence on a small set of platforms, providers, and security frameworks. It is this hidden concentration of power and vulnerability that sets the stage for the crisis this committee will explore.

The Rise of Microsoft and Crowdstrike

To understand the scale of the July 2024 outage, one must also understand how two companies—Microsoft and CrowdStrike—came to occupy such central positions in the digital ecosystem. Their trajectories from niche tech players to global digital gatekeepers are not just corporate success stories; they are case studies in how modern infrastructure has become increasingly consolidated in the hands of a few.[1]

Founded in 1975 by Bill Gates and Paul Allen, Microsoft began as a scrappy software company that built interpreters for early microcomputers. Its major breakthrough came in the 1980s, when it struck a deal with IBM to supply an operating system for personal computers. This was followed by the release of Windows, which quickly became the most dominant desktop

[1] Encyclopaedia Britannica. "Microsoft Corporation." *Encyclopaedia Britannica*. Last modified June 14, 2024. https://www.britannica.com/money/Microsoft-Corporation.

operating system by the 1990s. But what began as a product company soon evolved into something much larger. With the rise of the internet, Microsoft expanded aggressively into cloud computing, productivity software such as Microsoft Office, Teams, SharePoint, and enterprise infrastructure. By 2024, Microsoft Azure was the second largest cloud platform globally, used by over 95% of Fortune 500 companies to host critical operations ranging from healthcare to national defense.[2] Unlike traditional infrastructure (roads, electricity), Microsoft's dominance grew with relatively little regulation. As organizations digitized, they turned to Microsoft not just for tools, but for their entire backend architecture. Governments, militaries, and global corporations now depend on Microsoft to keep their core systems running—making the company less a vendor and more a digital utility. When Microsoft falters, the consequences are not isolated—they are global, systemic, and immediate.

Microsoft Office in Cologne, Germany.[3]

[2] Microsoft. "Microsoft Shares Strong Progress on Datacenter Region in Saudi Arabia; Construction Complete on Three Sites, with Availability Expected in 2026." *Microsoft News* (Middle East & Africa), December 4, 2024.
[3] *Microsoft Köln, RheinauArtOffice, Rheinauhafen Köln*. 2023. *FedScoop*. https://fedscoop.com/microsoft-launches-azure-openai-service-for-government/.

CrowdStrike, founded in 2011, was born in a very different digital era—one increasingly plagued by cyber threats. Its founders, George Kurtz and Dmitri Alperovitch, envisioned a new kind of cybersecurity platform: cloud-native, AI-driven, and proactive. By 2024, CrowdStrike had grown from a niche cybersecurity provider into a critical pillar of cyber defense, serving clients across sectors including finance, healthcare, aviation, and government. Microsoft itself uses CrowdStrike's Falcon platform to protect its own infrastructure and products.

This tight integration between the protector (CrowdStrike) and the provider (Microsoft) reflects a new kind of mutual interdependence in the tech world. Yet this also reveals great fragility: as more global systems rely on the same few security vendors, a single error—such as, say, a faulty CrowdStrike update—can ripple across every device, every institution, every region.

The Microsoft Megastructure

Microsoft Azure is the world's second-largest cloud platform, behind only Amazon Web Services (AWS). Azure powers everything from Netflix's streaming capabilities to the databases of European governments, enabling companies to run critical operations on virtual machines scattered across Microsoft's global data centers.

Windows still commands roughly 70.14% of the global desktop Operating System (OS) market.[4] Even many servers critical to finance, aviation, and logistics rely on Windows Server software. This means that when Microsoft updates a piece of code, the consequences ripple across nearly every sector of modern society. A flaw, a hack, or even an unintended bug can trigger systemic failures on a planetary scale.

[4] StatCounter Global Stats. "Desktop Operating System Market Share Worldwide." *StatCounter*. Accessed August 11, 2025. https://gs.statcounter.com/os-market-share/desktop/worldwide.

CrowdStrike: The Cybersecurity Web

Enter companies like CrowdStrike. While Microsoft builds and operates much of the digital scaffolding of the world, firms like CrowdStrike defend it. Founded in 2011, CrowdStrike pioneered the use of cloud-native endpoint protection.[5] Its flagship Falcon platform monitors millions of devices in real time, using machine learning to detect unusual patterns—stopping ransomware attacks before they encrypt hospitals, or isolating compromised laptops before malware jumps to sensitive corporate servers.

Microsoft is not just one of CrowdStrike's largest clients; the two are deeply integrated. CrowdStrike's tools run on top of Microsoft's operating systems and cloud servers. Likewise, CrowdStrike itself depends on major cloud providers (often including Azure) to deploy its detection and response systems. This interdependence is mirrored across countless companies.

Other critical players like Cisco and Palo Alto Networks fill in pieces of this vast digital defense puzzle, but the number of globally dominant security providers remains surprisingly small.[6] This means that any disruption in one corner of this ecosystem can cascade with alarming speed.

How We Became So Dependent

This consolidation did not happen by accident. Over the past two decades, organizations from airlines to municipal water utilities were urged to "modernize:" to shift away from aging local servers or paper systems and toward sleek cloud-hosted platforms. It was cheaper, faster,

[5] CrowdStrike. "CrowdStrike Investors Double Down and Lead $100 Million Series D Round to Support the Company's Global Growth." *CrowdStrike Blog*, May 16, 2017. https://www.crowdstrike.com/en-us/blog/crowdstrike-investors-double-down-and-lead-100-million-series-d-round-to-support-the-companys-global-growth/.

[6] Venture in Security. "20 Years of Cybersecurity Consolidation: How 200 Companies Became 11." *Venture in Security* (Substack), August 5, 2025. https://ventureinsecurity.net/p/20-years-of-cybersecurity-consolidation.

more scalable. A small logistics company in Portugal, for instance, could track shipments worldwide using Microsoft Dynamics. A hospital in Lagos could rent powerful digital health records systems without building its own IT fortress.

However, while this centralization fueled global growth and democratized digital power, it also increased risk. Today, nearly half of all global organizations rely on just two or three cybersecurity vendors. Over 80% of international financial institutions run at least part of their core operations on Microsoft or its direct competitors like AWS, often with shared dependencies.[7]

This interconnectedness means an attack on, or failure in, a single entity does not just disrupt one sector; it can paralyze hospitals, ground flights, freeze stock markets, and even compromise emergency services simultaneously.

The Rising Stakes of Cybersecurity

The frequency and sophistication of cyber threats have grown in parallel with this dependency. State-sponsored actors, criminal cartels, and lone hackers now target critical infrastructure not just for financial gain, but for espionage or geopolitical leverage.

In 2021, the Colonial Pipeline ransomware attack temporarily crippled nearly half of the fuel supply on the U.S. East Coast, causing panic buying and economic ripples. That same year, the SolarWinds attack (where hackers inserted malicious code into routine software updates) allowed intrusions into thousands of networks, including U.S. federal agencies and Fortune 500 firms.[8]

---

[7] Organisation for Economic Co-operation and Development (OECD). *Competition in the Provision of Cloud Computing Services.* OECD Roundtables on Competition Policy Papers No. 3 (2025). Paris: OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf.

[8] Cybersecurity and Infrastructure Security Agency (CISA). "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." *CISA News & Events*, May 7, 2023.

The growing reliance on companies like Microsoft and CrowdStrike to detect, mitigate, and recover from these attacks underscores how cybersecurity has become a pillar of modern public safety, on par with police or emergency medical services.

The Reality

This brings us back to the uncomfortable context for this committee. The world's digital infrastructure is, in many ways, remarkably fragile. It is propped up by a small group of software providers and cybersecurity firms, whose decisions on patching vulnerabilities or rolling out updates have global implications.

Moreover, the governance of this infrastructure is ambiguous and largely untested. Unlike roads, water, or electricity, which are typically overseen by national or municipal authorities, much of the world's digital "critical infrastructure" lies in the hands of very few companies. Who is ultimately responsible when systems fail? Who gets to decide how to restore services, prioritize regions, or allocate scarce cybersecurity resources during a crisis? Should private firms be allowed to dictate the pace of recovery after a breach, or should international bodies step in?

As the committee steps into the unfolding chaos of July 2024, these questions will shape every directive you draft and every alliance you forge.

Why Does This Matter?

Understanding this context is not just academic. It highlights why cooperation—between states, private companies, and international institutions—is both more difficult and more essential than ever before.

---

https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

Most of all, it reveals the stakes of your deliberations. In this committee, you will not simply be debating abstractions. You'll be grappling with how to secure hospitals where ventilators have stopped, how to keep air traffic control online so planes don't collide, and how to stabilize financial systems teetering on the edge of panic. You'll be forced to confront the consequences of a world built on a fragile foundation—and to chart a path forward when those pillars crack.

STATEMENT OF THE PROBLEM

Impacts on the Financial Sector

The CrowdStrike update crisis displayed the fragility of the global digital finance ecosystem. Even without malicious intent, it showed the world that servers, at home devices, and critical infrastructure can easily face systemic vulnerabilities.[9] From ATM networks and payroll processors, to broker-dealers and insurances, no component of the financial sector was left unscathed from the global power outage.

Disruptions to Retail and Commercial Banking

On July 19th, 2024, JPMorgan Chase reported that "a number of ATMs" went offline due to the CrowdStrike-related IT outage.[10] The organization confirmed that it was "actively working to restore the impacted machines." In Australia, both the Commonwealth Bank and National Australia Bank (NAB) experienced downtime in PayID instant transfers, ATM withdrawals, and merchant payments.[11] Several banks across the world reported similar issues. For instance, in India, banking officials reported that Windows terminals handling customer-facing operations like account queries, transactions, and "know your customer" verifications were rendered

[9] Fortinet. "What Is Endpoint Security?" Accessed August 14, 2025. https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security#:~:text=Endpoint%20security%20is%20the%20process,malware%20being%20installed%20on%20endpoints.
[10] Reuters. "JPMorgan Says Majority ATMs Operating Normally amid Outages." *Reuters*, July 19, 2024. https://www.reuters.com/business/finance/jpmorgan-says-majority-atms-operating-normally-amid-outages-2024-07-19/.
[11] Reuters. "What Disruptions Have Been Reported after Global Tech Outage?" *Reuters*, July 19, 2024. https://www.reuters.com/markets/commodities/what-disruptions-have-been-reported-after-global-tech-outage-2024-07-19/.

inoperable, leading to the temporary shutdown of numerous branches.[12] These issues led to disruption in individuals' abilities to purchase necessities and perform routine financial activities.

The New York Stock Exchange.[13]

Interruptions to Global Trading and Market Data

The London Stock Exchange Group (LSEG) publicly stated that its Workspace platform, which provides financial data including FX spot and forward market rates, suffered an outage early on July 19 before being restored later in the day.[14] Smaller broker-dealers in London and Singapore were also unable to transmit trades due to malfunctioning Windows terminals,

[12] Economic Times. "Banks in India Affected by Global Microsoft Outage." *The Economic Times*, July 19, 2024. https://economictimes.indiatimes.com/tech/technology/microsoft-outage.
[13] Benoist, Jean-Christophe. *NYC - New York Stock Exchange*. 2012. *Wikimedia Commons*.
[14] Reuters. "LSEG's Workspace Platform Suffers Outage, Market Sources Say." *Reuters*, July 19, 2024. https://www.reuters.com/technology/lsegs-workspace-platform-suffers-outage-market-sources-say-2024-07-19/.

reported Reuters.[15] In the U.S., trading platforms at Charles Schwab and E*Trade advised users not to submit duplicate orders after interface glitches were reported.[16] In an industry that works in fractions of a second, any delay is an issue; a global digital outage has dramatic consequences for traders.

Failures in ATM Networks and Payment Infrastructure

Across Europe and Australia, businesses were forced to temporarily switch to cash-only operations as Windows-based point-of-sale (POS) terminals and self-checkout kiosks displayed blue screen errors (Reuters).[17] In Australia, PayID, the popular instant payment system, went offline at multiple banks, highlighting endpoint dependency even within real-time payment infrastructures.[18] Every individual using non-cash payment, at every level, globally was impacted.

Impacts to Insurance, Payroll & Clearing Functions

Allianz, one of Europe's largest insurance firms, experienced employee login issues that interrupted back-end claims processing.[19] Though national clearing houses did not report major failures, multiple financial institutions indicated delays in overnight clearing operations due to locked or frozen workstations. While transactions themselves may not have been impacted, firms' abilities to execute them definitely were. This impacted payrolls, something millions of

[15] Reuters. "Traders in London and Singapore Struggle as Cyber Outage Disrupts Business." *Reuters*, July 19, 2024. https://www.reuters.com/technology/traders-london-singapore-struggle-cyber-outage-disrupts-business-2024-07-19/.
[16] Ibid.
[17] Reuters. "Global Tech Outage Delays Flights, Disrupts Services around World." *Reuters*, July 19, 2024. https://www.reuters.com/business/aerospace-defense/global-tech-outage-delays-flights-disrupts-services-around-world-2024-07-19/.
[18] Reuters. "What Disruptions Have Been Reported after Global Tech Outage?" *Reuters*, July 19, 2024. https://www.reuters.com/markets/commodities/what-disruptions-have-been-reported-after-global-tech-outage-2024-07-19/.
[19] Ibid.

employees depend on getting on a timely basis, too. Automatic Data Processing (ADP), a leading global payroll firm, acknowledged disruptions that delayed Friday payroll processing, affecting thousands of employers globally.[20]

Security Implications & Speculative Risk

While CrowdStrike confirmed the outage was not a cyberattack, cybersecurity officials from CISA and private sector analysts warned that the confusion "provided ideal conditions" for threat actors to launch phishing and spoofing campaigns.[21] Experts speculated that, had the defective update included a malicious payload, it could have led to data exfiltration or fraudulent financial transactions, turning a technical failure into a global cyber event.[22] These are severe, long term threats that still do not have a solution.

Moreover, this event undermined investor confidence in CrowdStrike, having long term implications for the company's stock performance. Financial regulators have since urged firms to implement "canary" testing, redundant fallback systems, and tighter endpoint segmentation to avoid similar system-wide failures.[23,24]

---

[20] Ibid.
[21] Reuters. "CrowdStrike Deploys Fix for Issue Causing Global Tech Outage." *Reuters*, July 19, 2024. https://www.reuters.com/technology/crowdstrike-says-actively-working-with-customers-impacted-by-outage-2024-07-19/
[22] Bloomberg. "CrowdStrike Earnings Beat Estimates in First Report after Cuts." *Bloomberg*, June 3, 2025. https://www.bloomberg.com/news/articles/2025-06-03/crowdstrike-earnings-beats-estimates-in-first-report-after-cuts?embedded-checkout=true.
[23] TechTarget. "What Is Canary Testing?" *TechTarget*, August 31, 2022. Published by Rahul Awati and Peter Loshin. https://www.techtarget.com/whatis/definition/canary-canary-testing
[24] Dexon Systems. "Redundant Systems: Definition, Types, and Use Cases." Accessed August 14, 2025. https://dexonsystems.com/blog/redundant-systems.

Impact on Supply Chains

The global Microsoft outage disrupted key cloud-based services, including Azure, Teams, Outlook, and OneDrive. These services form the backbone of digital infrastructure across multiple industries and are heavily integrated into logistics, inventory management, and day-to-day operations. As a result, the outage caused widespread delays and breakdowns in global supply chains.[25]

Communication failures between suppliers, manufacturers, and distributors prevented coordination of shipments and deliveries. Many firms lost access to critical scheduling and inventory platforms, halting production and leading to inventory backlogs or shortages.[26] Port authorities and freight operators reported failure in cargo tracking and routing systems, compounding logistical gridlock. Air cargo operations were also severely affected, as disruptions in flight scheduling and routing systems grounded or delayed planes, further slowing the movement of time-sensitive goods such as medical supplies, electronics, and perishable products. This bottleneck in air transport created a ripple effect across international supply networks, intensifying shortages and extending delivery timelines.[27] Industries that rely on just-in-time production models, such as the automotive industry—where goods are produced as needed rather than stockpiled—experienced severe disruptions due to their reliance on real-time cloud-based planning tools.[28]

---

[25] www.ETManufacturing.in. "Microsoft Outage: How the Global Outage Affected the Manufacturing Industry? Uncovers Cloud Dependency Risks - et Manufacturing." *ETManufacturing.In*, 20 July 2024, manufacturing.economictimes.indiatimes.com/news/industry/microsoft-outage-how-the-global-outage-affected-the-manufacturing-industry-uncovers-cloud-dependency-risks/111881325#:~:text=Many%20manufacturing%20companies%20rely%20on,risk%20of%20mistakes%20and%20inefficiencies.

[26] Ibid.

[27] Lori Ann LaRocco. "Microsoft, Crowdstrike It Outage Hits Global Supply Chain, with Air Freight Facing Days or Weeks to Recover." *CNBC*, CNBC, 19 July 2024, www.cnbc.com/2024/07/19/crowdstrike-it-outage-spreads-global-supply-chain.html.

[28] *Tesla Halted Some Production Lines Due to Global It Outage, Business Insider Reports | Reuters*, www.reuters.com/business/autos-transportation/tesla-halted-some-production-lines-due-global-it-outage-business-insider-reports-2024-07-19/. Accessed 16 June 2025.

The outage also highlighted disparities in digital preparedness. While larger corporations were able to implement contingency measures or switch to alternative platforms, small and mid-sized enterprises with limited IT resources were disproportionately affected.[29] The incident exposed a structural imbalance in global trade: while larger firms could absorb the shock, smaller enterprises were left without the tools or support to adapt, deepening existing digital and operational divides.

As the committee responds to the consequences of this outage, it must address both the short-term recovery of affected supply chains and the long-term need for more resilient and diversified technological infrastructure.

Governing Critical Infrastructure

The Microsoft outage also exposed major vulnerabilities in how governments operate and protect critical infrastructure. As Microsoft cloud services failed, so did many essential public systems that depend on them, including emergency dispatch, law enforcement databases, border control operations, and public transportation networks.

[29] D'Innocenzio, Anne, and Haleluya Hadero. "Many Small Businesses Struggle to Resume Normal Operations Days after Global Tech Outage." *PBS*, Public Broadcasting Service, 21 July 2024, www.pbs.org/newshour/economy/many-small-businesses-struggle-to-resume-normal-operations-days-after-global-tech-outage.

Long crossing at the US-Canada border.[30]

In the United States, 911 emergency dispatch systems in multiple cities temporarily went offline.[31] Furthermore, dispatchers were unable to access driving and criminal records, raising serious public safety concerns.[32] At both the U.S.-Canada and U.S.-Mexico borders, long delays were reported, with some individuals unable to cross for work.[33] In various cities, commuters were affected as real-time arrival information became unavailable.[34] This raises urgent questions about how much control governments truly have over the digital infrastructure that underpins public services.

---

[30] *Border Crossing into US*. 2007. *Flickr*, Peace Bridge, Buffalo, NY, https://www.flickr.com/photos/chapstickaddict/973379513.
[31] Burga, Solcyré. "Here Are the States Is 911 Impacted Due to the Tech Outage." *Time*, Time, 19 July 2024, time.com/7000621/911-impacted-microsoft-outage/.
[32] "Microsoft Outages Affecting Dispatch Centers across the Country." *FireRescue1*, FireRescue1, 19 July 2024, www.firerescue1.com/911-and-dispatch/microsoft-outages-affecting-dispatch-centers-across-the-country.
[33] *Microsoft It Outage: Border Crossings into the U.S. Delayed by the Internet Disruption*, nationalpost.com/news/world/microsoft-it-outage-updates. Accessed 17 June 2025.
[34] Dean, Grace. "Commuters in NYC and DC Should Get Ready for a Difficult, Disrupted Journey Due to the Global It Outage." *Business Insider*, Business Insider, www.businessinsider.com/nyc-dc-subway-global-it-outage-crowdstrike-new-york-washington-2024-7. Accessed 16 June 2025.

The outage demonstrated how deeply governments have integrated private sector technology into their most sensitive operations. Many agencies lacked independent backups or clear emergency protocols when these systems failed. The incident highlighted not just the fragility of digital systems, but also the absence of strong oversight, coordination, and contingency planning.

This committee must now consider how to ensure that governments can maintain essential services in the face of digital breakdowns. Should governments invest in their own infrastructure? Should there be stricter rules for private technology vendors? And how can national security and public safety be protected when vital systems depend on platforms beyond government control?

Impact on Aviation

The global Microsoft outage unleashed a severe and immediate crisis in the aviation sector, revealing just how deeply airlines, airports, regulatory bodies, and logistics companies depend on interconnected digital systems, many of which are built on or integrated with Microsoft's platforms. From passenger check-ins to air traffic control coordination, the outage disrupted nearly every layer of modern aviation, threatening not only economic stability but passenger safety.

The Collapse of Digital Coordination

At the core of the disruption was the sudden loss of access to critical cloud-based services that underpin nearly every aspect of aviation operations. The aviation industry has leaned heavily into digital transformation over the last decade; the aviation sector continues its rapid digital

transformation. A recent Aviation Cloud Market analysis estimates the market at $6.1 billion in 2024, expected to more than double to $12.9 billion by 2029, reflecting soaring adoption of cloud-based systems across airlines.[35]

Passenger processing ground to a halt. On a typical day, airports worldwide handle over 12 million passengers, and with check-in systems, boarding pass issuance, and baggage routing tied to Microsoft-based platforms, terminals quickly descended into chaos.[36] Airports from London Heathrow to Chicago O'Hare reported average delays stretching 4 to 6 hours, as airline staff scrambled to switch to cumbersome manual processing or simply cancelled flights when overwhelmed.

The situation was exacerbated by the collapse of global airline alliances, stranding travelers and aircraft in mismatched locations across the world and creating logistical headaches that rippled for days. Meanwhile, many aircraft sat idle on tarmacs because airlines could not access digital maintenance logs.

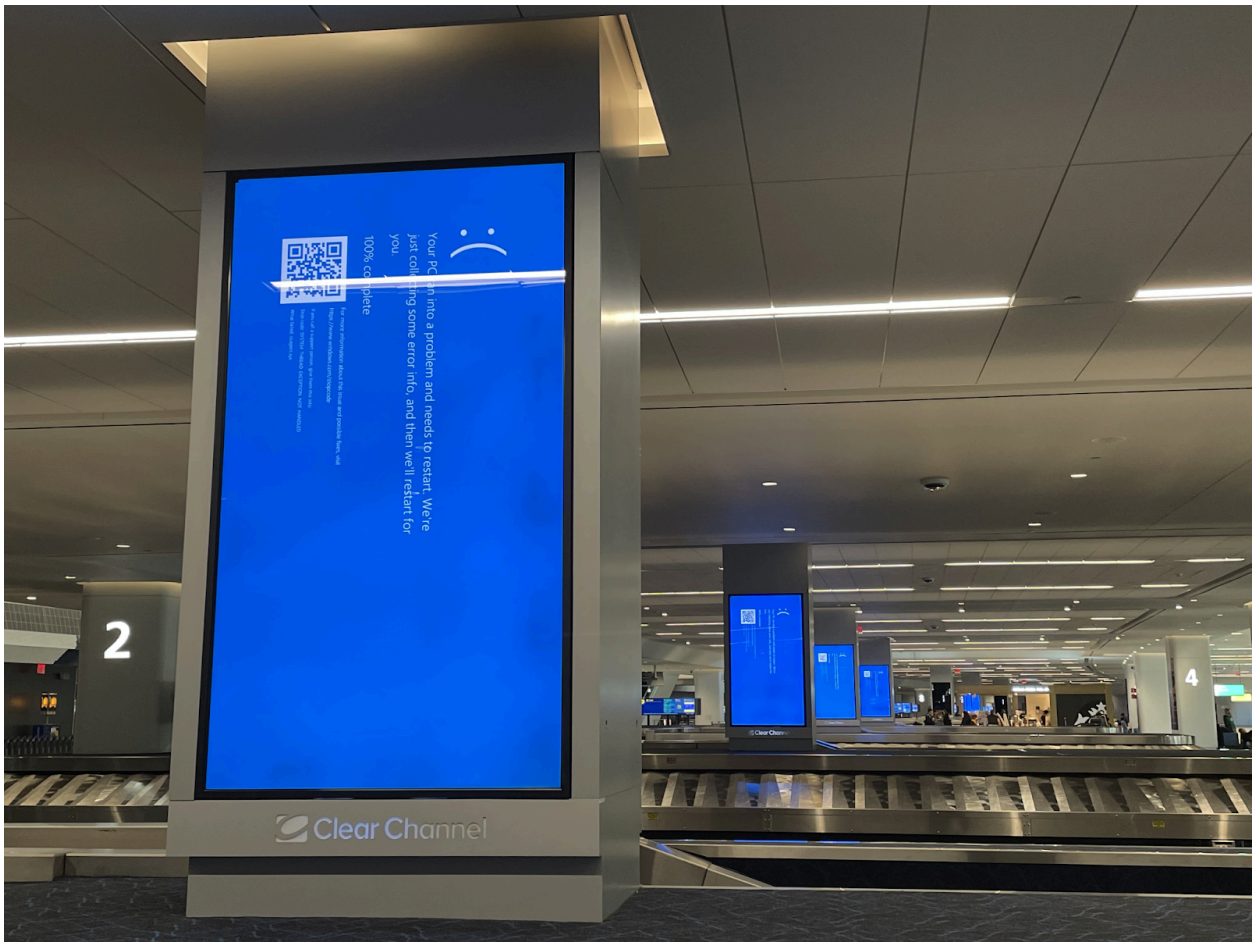
Threats to Air Traffic Control and Flight Safety

Perhaps most alarming was the strain on air traffic management. While core radar and radio communications networks typically run on highly secured, independent systems, many vital support tools, such as flight plan databases, advanced weather visualizations, and inter-airport coordination platforms, are hosted on or are deeply integrated with Microsoft's infrastructure. The sudden outage of these systems forced airports and controllers to enact immediate, sweeping changes.

---

[35] ePlaneAI. "The Impact of AI on the Aviation Cloud Market." ePlaneAI, June 9, 2025. (Accessed via supplemental summary).

[36] CNBC, "Here Are the Top 15 Busiest Airports in the World," *CNBC*, July 8, 2025, accessed August 11, 2025, https://www.cnbc.com/2025/07/08/here-are-the-top-15-busiest-airports-in-the-world.html#:~:text=Hartsfield%2DJackson%20Atlanta%20International%20Airport,billion%20people%20traveling%20by%20air.



"Blue Screen of Death" at LaGuardia Airport, July 19 2024.[37]

Globally, over 100–130,000 flight plans are processed daily, with major hubs like Atlanta, Frankfurt, and Dubai.[38] During the outage, processing delays and lost data meant many airports were compelled to reduce their capacity, slashing the number of flights that could safely depart or land. Real-time weather data feeds, crucial for dynamic routing around storms or turbulence, were also severely disrupted. Lacking updated forecasts, airlines adopted a

[37] Smishra1. *CrowdStrike BSOD at LGA*. July 19, 2024. *Wikimedia Commons*. https://upload.wikimedia.org/wikipedia/commons/9/94/CrowdStrike_BSOD_at_LGA.jpg.
[38] EAS Barcelona, "How Many Planes Fly per Day Around the World," *EAS Barcelona*, accessed August 11, 2025, https://easbcn.com/en/how-many-planes-fly-per-day-around-the-world/#:~:text=Global%20air%20traffic%20is%20one%20of%20the,100%2C000%20and%20130%2C000%20flights%20per%20day%20worldwid.

conservative approach, which led to a reduction in transatlantic departures on the worst days, according to Eurocontrol figures.

Equally concerning was the impact on cross-border coordination. Under normal circumstances, data from one nation's air traffic control seamlessly transitions to another's via digital handoffs, maintaining tight aircraft separation in busy corridors. But with automated systems offline, controllers were forced to rely on manual phone coordination, drastically reducing throughput and adding hours to flight times. Although no midair incidents occurred, this was largely due to these emergency measures, underscoring just how close the system came to operational paralysis.

A Logistical and Economic Disaster

The immediate economic toll on aviation was catastrophic. While the International Air Transport Association (IATA) hasn't published a precise daily loss metric for reductions in capacity, it's well-known that airline profitability is highly sensitive to flight operations disruptions. Even modest capacity cuts translate into substantial financial losses, often running into the millions of dollars per day, especially when factoring in lost fares, compensation, and operational inefficiencies. With the outage cutting capacity, airlines lost over $800 million in direct revenue within just three days, excluding secondary impacts.[39] These additional costs, ranging from passenger compensation to hotel accommodations for stranded travelers pushed the combined immediate financial blow past the $5.4 billion mark.[40]

[39] CIO Dive, "CrowdStrike Disruption Direct Losses to Reach $5.4 B for Fortune 500, Study Finds," *CIO Dive*, July 25, 2024, accessed August 11, 2025, https://www.ciodive.com/news/crowdstrike-cost-fortune-500-losses-cyber-insurance/722463/.
[40] Ibid.

The disruption was not limited to passenger operations. Warehouses at major hubs quickly overflowed. Pharmaceutical shipments, high-value electronics, and even some critical vaccine batches missed temperature-sensitive transit windows, highlighting the high stakes of aviation's dependency on continuous digital coordination.

Complex disputes arose over whether the outage constituted a cyber event covered under standard aviation policies, and who ultimately bore responsibility: the airlines that adopted these systems, the technology vendors whose platforms failed, or even government regulators who encouraged widespread digital migration without enforcing stronger safeguards.

Exposing Structural Vulnerabilities in Aviation IT

This crisis did not merely reveal operational disarray; it laid bare deep structural weaknesses in the aviation sector's embrace of cloud technology. When Microsoft's networks suffered cascading failures, there were few independent fallback systems left.

Despite years of industry rhetoric about redundancy and business continuity, very few airlines maintain comprehensive offline backups of essential operations data. For many, the cost and complexity of synchronizing live passenger, maintenance, and scheduling data across redundant platforms proved prohibitive, a gamble that backfired spectacularly during the outage.

What the Committee Must Consider

This outage forces a reckoning with how aviation balances its drive for seamless digital efficiency against the risk of systemic collapse. This is no longer an abstract concern. With over 100,000 flights disrupted, tens of millions of passengers impacted, and billions in losses within mere days, this crisis demonstrated that a single software flaw or cyber breach can achieve what storms, labor strikes, or even geopolitical conflicts rarely have: grounding the global fleet.

As this committee responds to the aftermath of the outage, it faces decisions that will shape not only the recovery of the aviation sector, but its very architecture in the years ahead. Key questions demand your attention.

How can the aviation industry reduce its overwhelming dependence on a handful of digital providers? Should international bodies like the International Civil Aviation Organization (ICAO) or IATA introduce regulations mandating that critical systems be platform-agnostic or operate across multiple cloud infrastructures? Should there be enforceable global standards for maintaining offline backups, with audits to ensure compliance - and penalties for neglect?

What about the cybersecurity firms like CrowdStrike, whose advanced detection systems are deeply integrated into these aviation IT environments? Does the current model place too much reliance on their judgment and threat intelligence? Should aviation authorities form direct strategic partnerships with such firms, establishing joint protocols that clearly define responsibilities and liabilities in crises of this magnitude?

The committee must also grapple with protecting smaller carriers and airports. Many airlines worldwide are small or midsize, often lacking the resources to invest in sophisticated cybersecurity or redundant IT systems. Should there be an international aviation resilience fund, contributed to by major airlines and tech giants, to help sustain the entire global network?

Recovery

By July 20, services were gradually returning to functionality across multiple sectors, after CrowdStrike and Microsoft implemented a corrective patch for the faulty update.[41] They

[41] Reuters. "Microsoft Says about 8.5 Million of Its Devices Affected by CrowdStrike-Related Outage." *Reuters*, July 20, 2024. https://www.reuters.com/technology/microsoft-says-about-85-million-its-devices-affected-by-crowdstrike-related-2024-07-20/.

released a recovery script and detailed guidance on rebooting affected machines.[42] However, recovery took longer than expected: according to experts from Security Scorecard, many affected Windows systems required manual reboots and removal of the problematic update, meaning that full restoration often extended over 48–72 hours.[43]

As Delegates of the Outage Outrage, it is your responsibility to take note of the discussed concerns and take the first steps towards detailing long term solutions to protect critical infrastructure. For a bit of direction, know that industry leaders across affected sectors are urging the adoption of new policy frameworks that include: mandatory downtime drills, regulatory requirements for endpoint resilience, and updated liability mechanisms to ensure software providers like CrowdStrike and Microsoft can be held accountable for systemic incidents. As you prepare for Committee, remember your objective to make our fragile digital landscape safer.

[42] Reuters. "CrowdStrike Update That Caused Global Outage Likely Skipped Checks, Experts Say." *Reuters*, July 20, 2024. https://www.reuters.com/technology/cybersecurity/crowdstrike-update-that-caused-global-outage-likely-skipped-checks-experts-say-2024-07-20/.
[43] Ibid.

Delegate Positions

Michael Kratsios (CTO of the United States of America)

Michael has spent his career working at the intersection of government and innovation, focused on ensuring that the United States doesn't just adapt to emerging technologies, but leads their development with responsibility. As Chief Technology Officer, he plays a key role in shaping national strategy on AI, cybersecurity, digital infrastructure, and tech-driven public services. In the face of the outage crisis, his attention is firmly on the nation's financial infrastructure—the complex, high-speed network that underpins the global economy and touches nearly every American life. He views a breakdown here not just as a technical failure, but as a direct threat to national security and economic stability. Known for his calm and deliberate approach, Michael is often described as cautious, but deeply principled: a policymaker who believes in both innovation and preparation. In his free time, he jogs through national parks to disconnect and clear his mind. He's also an avid reader of science fiction, drawn to stories that challenge the assumptions of the present. Beneath his steady exterior is a strategist who understands that the future can't be delayed and that resilience must be built before it's tested.

David Knott (CTO of the United Kingdom)

David Knott has spent over three decades navigating complex digital transformations across sectors including banking, transport, and utilities. Now serving as the UK Government's Chief Technology Officer, he leads efforts to modernize public sector technology, replace legacy systems, and embed ethical, scalable architecture across departments. His primary concern lies in the resilience of the supply chain infrastructure; a tightly interwoven network of ports, freight,

and digital logistics that keeps the UK economy moving. He sees any instability here not merely as a technical inconvenience, but as a national vulnerability with wide-reaching economic and social impacts. Known for his composed, systems-oriented mindset, David believes effective digital leadership requires both precision and patience. In his free time, he enjoys kayaking along the British coast, where the rhythm of the water contrasts with the pace of Whitehall. He also writes regularly about leadership and AI ethics, reflecting a habit of thinking long-term even in short-term crises. David brings a quiet conviction to his work: that true digital transformation is not about speed, but about lasting stability.

Maxut Shadayev (Deputy Minister of Digital Development, Russian Federation)

Maxut Shadayev has led Russia's digital modernization efforts with a focus on strengthening national technological autonomy and reducing reliance on foreign platforms. As Minister, he oversees the development of digital infrastructure, cybersecurity strategy, and the broader coordination of Russia's information systems. His primary concern lies with the healthcare infrastructure, which has increasingly relied on digitized patient data, remote diagnostics, and centralized medical records across the country. To Maxut, any vulnerability in this system poses not only operational risks, but also challenges to public trust and state resilience. He is known for his pragmatic, strategic mindset, prioritizing control, continuity, and the development of domestic solutions over rapid innovation. In his personal life, Maxut enjoys distance running, often using it as a time for reflection and mental clarity. He also collects Soviet-era radio equipment, a nod to his interest in the evolution of communication technology.

His leadership reflects a deep belief in sovereignty through self-sufficiency. Digital strength, in his view, must be built from within.

Yin Hejun (Minister of Science and Technology, People's Republic of China)

Yin Hejun is a seasoned engineer-turned-politician who now leads China's national strategy for technological independence and innovation. As Minister of Science and Technology, he spearheads China's drive toward self-reliance in AI, semiconductors, quantum computing, and supercomputing infrastructure. His greatest concern is the resilience of industrial supply chain infrastructure, especially the networks linking manufacturing hubs, power systems, and data centers that form the backbone of the digital economy. He sees disruption in this area not merely as an operational hiccup, but as a strategic threat to economic continuity and national technological momentum. Known for his methodical, long-range thinking and adherence to centralized coordination, Yin emphasizes state-led planning, combined with high standards in data governance. In his personal time, he practices tai chi at dawn: a practice that reflects his balance between tradition and modern strategy. He also enjoys studying vintage computer hardware, reflecting his fascination with the roots of digital evolution. Yin brings to the fore a leadership style rooted in discipline, foresight, and the conviction that technological resilience must precede disruptive ambition.

Clara Chappaz (Minister Delegate for Artificial Intelligence and Digital Technologies, France)

Clara Chappaz has risen through the ranks of France's digital ecosystem, from leading French Tech initiatives to her current role as Minister Delegate overseeing AI and digital technologies. In her position, she shapes France's strategic trajectory on AI governance, data sovereignty, and public sector digital transformation. Her main concern centers on the resilience of government digital services infrastructure - the platforms underpinning citizen services, administrative processes, and public data exchange. She sees disruption in this area not simply as a technical issue, but as a threat to civic trust and democratic function. Known for being forward-thinking and citizen-centric, Clara emphasizes transparency in digital policy, user experience, and responsible innovation. In her free time, she enjoys urban gardening on her Paris balcony, finding metaphor in nurturing small ecosystems. She also composes electronic music, blending structure with creativity, a subtle reflection of her policy style. Clara represents a vision of leadership grounded in collaboration, reliability, and the conviction that technology must serve people first.

S. Krishnan (Secretary, Ministry of Electronics & Information Technology, India)

S. Krishnan brings decades of experience in public service to his role as Secretary of MeitY, where he oversees India's digital architecture, cybersecurity frameworks, and regulatory strategy. A key architect of the country's push toward digital public infrastructure, Krishnan has focused on building systems that are scalable, inclusive, and sovereign. His chief concern lies with the integrity of financial infrastructure: the dense web of real-time payments, digital

banking, and identity-linked transactions that supports daily economic activity for over a billion people. He views disruptions in this system not just as technical incidents, but also risks to livelihoods, social stability, and economic momentum. Calm and measured in his approach, Krishnan is known for his emphasis on long-term capacity-building over short-term fixes. In his personal life, he enjoys long evening walks through his neighborhood, using the time to reflect and disconnect. He also finds joy in cooking traditional South Indian dishes, appreciating the quiet discipline of preparing food from scratch. His leadership is grounded in the belief that digital systems must be resilient not just in design, but in how they serve the most ordinary moments of daily life.

Shaza Fatima Khawaja (Federal Minister for Information Technology & Telecommunication, Pakistan)

Shaza Fatima Khawaja leads Pakistan's digital development strategy as Federal Minister for Information Technology and Telecommunication, where she oversees key national initiatives in cybersecurity, e-governance, and digital access. With a background in economics and public policy, she brings a people-centered lens to tech policy, emphasizing inclusion, innovation, and resilience. Her primary concern lies with the financial infrastructure—the expanding network of mobile wallets, digital banking services, and interbank platforms that power Pakistan's everyday economy. She views any disruption in this system as not just a technical issue, but a direct blow to economic stability and public confidence. Known for her sharp communication skills and forward-thinking mindset, Shaza balances long-term ambition with political agility. In her spare time, she enjoys oil painting, often creating abstract works that reflect the tensions and harmonies of change. She also writes Urdu poetry, finding in language the same precision and

rhythm she seeks in policy. Her leadership is rooted in the belief that digital transformation must be built on systems that are not only modern, but trusted and durable.

Andrew Morrison (CTO of Australia)

Andrew Morrison serves as the Chief Technology Officer of Australia's Digital Transformation Agency, where he leads the design and implementation of digital platforms and standards across the federal government. With a background in systems engineering and public sector innovation, he is responsible for modernizing service delivery while maintaining resilience across critical digital infrastructure. His core concern is the stability of financial infrastructure, specifically the government-linked identity systems and payment rails that enable welfare disbursement, tax operations, and real-time digital services. To Andrew, failure in this domain is not just a technical concern, but a disruption to public trust and institutional reliability. Known for his calm demeanor and structured problem-solving, he brings a steady hand to high-pressure decision-making. Outside of work, he is an avid surfer, drawn to the clarity and unpredictability of the ocean. He also plays classical guitar, appreciating the discipline it demands and the space it gives him to think creatively. His leadership is grounded in the principle that technology must work quietly and reliably in the background, especially when the stakes are highest.

Dr. Amr Talaat (Minister of Communications and Information Technology, Egypt)

Dr. Amr Talaat serves as Egypt's Minister of Communications and Information Technology, where he oversees the country's national digital strategy, infrastructure security, and technological innovation agenda. With a background in telecommunications and a doctorate in

information systems, he has led Egypt's transition toward digital governance while expanding broadband access and smart service delivery across urban and rural sectors alike. His foremost priority is protecting the systems that support Suez Canal operations—especially the digital logistics, customs, and maritime traffic platforms that underpin Egypt's trade economy. To Dr. Talaat, resilience in this domain is not just economic—it is geopolitical, shaping Egypt's role as a regional gateway between continents. Known for his methodical decision-making and deep technical fluency, he brings a balance of realism and long-term vision to multilateral cooperation. Outside of his ministerial duties, he is an amateur pianist and a keen student of classical Arabic poetry, both of which, he says, sharpen his focus and remind him of the value of structure in chaos. His leadership reflects a belief that digital infrastructure should be quiet, seamless, and strategically sovereign.

Dr. Belete Molla (Minister of Innovation and Technology, Ethiopia)

Dr. Belete Molla serves as Ethiopia's Minister of Innovation and Technology, where he oversees the development and integration of digital systems across key public sectors. With a background in engineering and a career rooted in research and science policy, he has championed Ethiopia's push to expand digital access, promote homegrown innovation, and close infrastructure gaps between rural and urban communities. His primary concern is the stability of digital healthcare systems, particularly those enabling disease surveillance, rural telemedicine, and electronic medical record networks. In Ethiopia, where healthcare access remains uneven, he sees digital tools not as luxuries but as necessities to deliver timely, life-saving care. Dr. Molla is known for his pragmatic leadership and steady focus on long-term institutional resilience. He often reminds his team that technology policy must be grounded in human realities, not abstract

metrics. Beyond government, he enjoys landscape photography and tending to his herb garden, which he credits with teaching him patience and attention to detail. His vision is clear: build systems that are not only smart but also enduring, inclusive, and trusted.

Dr. Toshiko Abe (Minister of Education, Culture, Sports, Science and Technology, Japan)

Toshiko Abe serves as Japan's Minister of Education, Culture, Sports, Science and Technology, where she oversees the country's national strategies for scientific advancement, research innovation, and digital education. With a background in medicine and a long-standing career in public service, she has been a key voice in strengthening Japan's position as a leader in high-tech research and resilient knowledge infrastructure. Her top priority is ensuring the integrity and security of Japan's national research systems - particularly those tied to health data, climate modeling, and advanced computing. For Minister Abe, disruption to scientific infrastructure is not just a threat to innovation, but a direct risk to public health, economic competitiveness, and social cohesion. Known for her composed, forward-thinking approach, she advocates for robust digital autonomy while maintaining deep international research partnerships. Outside of government, she enjoys traditional Noh theater and practices ikebana, the Japanese art of floral arrangement—both disciplines that reflect her belief in balance, precision, and quiet strength. Her leadership is driven by the conviction that science, culture, and technology must evolve together to build a future that is both secure and humane.

Jiraporn Sindhuprai (Minister of Higher Education, Science, Research, and Innovation, Thailand)

Jiraporn Sindhuprai serves as Thailand's Minister of Higher Education, Science, Research and Innovation, where she leads national efforts to strengthen scientific capacity, expand digital research infrastructure, and guide the country's emerging technology policy. With a background in law and a career spanning both legislative and academic leadership, she has played a pivotal role in aligning Thailand's digital ambitions with its educational and economic priorities. Her central focus is protecting the systems that support national research networks, particularly those that connect universities, laboratories, and public health institutions across provinces. In Thailand, where research informs pandemic response, agricultural forecasting, and rural development, the integrity of scientific data infrastructure is a matter of national resilience. And, as a nexus of Eastern tourism, the Kingdom is deeply concerned about the chaos caused when airline alliances fell apart due to their shared communication systems all going down at once. Minister Jiraporn is known for her direct communication style and her ability to navigate both political and technical environments with clarity. She believes digital transformation must be both equitable and context-sensitive, especially in a region as diverse as Southeast Asia. Outside her role, she enjoys watercolor painting and Muay Thai, appreciating both for their rhythm, discipline, and connection to Thai cultural identity. Her leadership reflects a commitment to innovation that is deeply rooted in place, people, and purpose.

Dorothee Bar (Minister for Research, Technology, and Space, Germany)

Dorothee Bär serves as Germany's Minister for Research, Technology, and Space, and leads the country's newly established Ministry for the Future, a strategic initiative focused on long-term digital resilience, climate innovation, and space policy. With a background in political science and a longstanding focus on digital affairs, she is widely known as one of Germany's most vocal advocates for technological modernization across public and private sectors. Her central concern is the protection of energy infrastructure, particularly the smart grids, hydrogen systems, and cross-border data platforms that underpin Germany's transition to a sustainable, digitally integrated economy. For Minister Bär, a disruption to this infrastructure threatens not only domestic stability, but Europe's broader efforts toward green reindustrialization and energy sovereignty. She is known for her forward-looking leadership style and her ability to link emerging technologies with practical governance. Passionate about youth engagement and STEM education, she often emphasizes the need to make complex systems legible and accessible to future generations. Outside her work, she is an amateur drone pilot and a collector of vintage science fiction novels, both interests that reflect her fascination with future worlds. Her vision is one of pragmatic optimism: build now, anticipate later, and design systems that can withstand what we don't yet see coming.

Eng. Abdullah Amer Alswaha (Minister for Communications and Information Technology, Saudi Arabia)

H.E. Eng. Abdullah Amer Alswaha serves as Saudi Arabia's Minister of Communications and Information Technology, where he leads the Kingdom's ambitious digital transformation

agenda and oversees national strategies in AI, cybersecurity, and emerging technologies. With a background in electrical engineering and global executive experience in the tech sector, he has been a central figure in modernizing Saudi Arabia's digital infrastructure under Vision 2030. His key priority is the resilience of digital government services, including identity systems, service portals, and cloud platforms that connect millions of citizens to health, education, and welfare programs. For Minister Alswaha, stability in this domain is essential to building trust between the state and society in a rapidly digitizing world. He is known for his energetic leadership style and his ability to bridge global innovation trends with local development goals. A strong advocate for public-private collaboration, he often emphasizes agility, cybersecurity, and talent development as pillars of national resilience. Outside of his official role, he enjoys falconry and long-distance cycling—both of which, he says, remind him of the importance of vision, discipline, and adaptability in navigating complex terrain. His leadership reflects Saudi Arabia's effort to reimagine its future through technology: secure, citizen-centered, and globally competitive.

Karin Keller-Sutter (Federal Councillor overseeing the Federal Department of Finance, Switzerland)

Karin Keller-Sutter serves as Switzerland's Federal Councillor overseeing the Federal Department of Finance, which includes responsibility for the Federal Office of Information Technology, Systems and Telecommunication (FOITT). With a background in economics and law, she brings a precise and institutionally grounded perspective to national digital policy. Her focus lies in safeguarding Switzerland's financial infrastructure, particularly the digital systems that underpin real-time banking, secure data exchange, and public trust in the federation's

decentralized governance. In a country renowned for neutrality and discretion, the stability of financial and information networks is treated as a matter of sovereignty and national identity. Councillor Keller-Sutter is known for her no-nonsense leadership style and her ability to bridge complex regulatory frameworks with practical digital reforms. She often emphasizes digital resilience as a form of civil defense, essential to protecting both the economy and democratic institutions. Outside of office, she is a lifelong pianist and an avid mountaineer, drawn to activities that demand both discipline and quiet strategic thinking. Her approach to technology is measured and pragmatic, anchored in the belief that in Switzerland, digital security is not just a tool, but a national principle.

Dr. Eduardo Ortega-Barria (CTO of Panama)

Dr. Eduardo Ortega-Barría serves as Panama's National Secretary of Science, Technology, and Innovation, where he leads the National Secretariat of Science, Technology, and Innovation (SENACYT). A physician and immunologist by training, he brings decades of experience in biomedical research and global health policy to his role advancing Panama's digital and scientific capabilities. His top priority is strengthening the digital foundations of public health and research—particularly platforms for disease surveillance, medical data integration, and emergency response coordination. In Panama, where healthcare and research institutions play a vital role in managing both tropical disease risks and cross-border public health efforts, the stability of these systems is critical to social trust and regional leadership. The government he represents, of course, is also deeply concerned with ensuring that all impacts on global trade from this crisis are miniscule and that he can help formulate some preventative medicine against trade chaos in the future. Dr. Ortega-Barría is known for his methodical,

evidence-driven approach and his commitment to building scientific capacity through education, innovation, and strategic partnerships. He often emphasizes the importance of building systems that serve both researchers and communities. Outside of government, he is an amateur ornithologist and enjoys playing the cello, hobbies that reflect both curiosity and discipline. His leadership style is grounded in the belief that science and technology must be woven into the fabric of public life, not layered on top of it.

Mehmet Fatih Kacır (Minister of Industry and Technology, Türkiye)

Mehmet Fatih Kacır serves as the Minister of Industry and Technology in Türkiye, where he oversees national strategies on industrial digitization, advanced manufacturing, and technological self-sufficiency. With a background in mechanical engineering and a career spanning entrepreneurship, innovation policy, and institutional reform, he has been a central figure in Türkiye's push to position itself as a regional technology hub. His primary focus is ensuring the continuity of digital supply chains and smart industrial platforms—particularly those that link Türkiye's automotive, defense, and logistics sectors to both domestic and international markets. For Minister Kacır, any breakdown in this infrastructure risks more than economic losses; it threatens Türkiye's strategic autonomy and role as a bridge between Europe, Asia, and the Middle East. He is known for his energetic, mission-driven leadership style and for championing youth innovation and public-private collaboration. He often speaks of technology as both a tool for national strength and a catalyst for generational transformation. Outside of office, he enjoys traditional Turkish calligraphy and restoring old bicycles, hobbies that reflect his appreciation for design, heritage, and purposeful engineering. His vision for Türkiye is one where resilience is built into every layer of the nation’s digital and industrial backbone.

Dr. Rosaura Ruiz Gutiérrez (Secretary of Science, Humanities, Technology and Innovation, Mexico)

Dr. Rosaura Ruiz Gutiérrez serves as Mexico's Secretary of Science, Humanities, Technology and Innovation, where she leads national efforts to integrate scientific research, digital policy, and humanistic inquiry into public development. A biologist, academic, and former dean of the Faculty of Sciences at the National Autonomous University of Mexico (UNAM), she brings decades of experience in education, gender equity, and research policy to her current role. Her central focus is on safeguarding the digital and institutional infrastructure that supports Mexico's public universities, research centers, and science education systems. In a country where access to knowledge is deeply linked to economic mobility and democratic inclusion, she views the protection of these systems as foundational to national resilience. Known for her principled leadership and sharp intellect, she emphasizes equity, public engagement, and long-term investment in people over short-term metrics. Outside of office, she is an avid reader of historical fiction and finds joy in caring for her rooftop garden in Mexico City, spaces where she finds both perspective and patience. Her vision for Mexico is rooted in the belief that technology must be guided by critical thought, and that progress must be both innovative and inclusive.

Óscar Lopez (Minister for Digital Transformation and Public Function, Spain)

Óscar López serves as Spain's Minister for Digital Transformation and Public Function, where he leads national initiatives focused on modernizing public administration, expanding digital services, and reinforcing cybersecurity across state infrastructure. With a background in

political science and years of experience in both regional and national governance, he has emerged as a key figure in Spain's efforts to bring public services closer to citizens through seamless, secure, and user-friendly digital platforms. His primary focus is the resilience of civic infrastructure, particularly Spain's digital identity systems, social security networks, and e-government portals that millions depend on daily. For Minister López, digital transformation is not just about efficiency—it's about strengthening democratic trust through reliable access, transparency, and inclusion. Known for his pragmatic and consensus-driven leadership style, he often brings together technical experts and civil society leaders to ensure that reforms remain grounded in public need. Outside of government, he is an avid cyclist and a lover of Spanish cinema, often drawing inspiration from stories that capture change at the human scale. His approach to leadership reflects a belief that strong institutions begin with well-designed, well-defended digital foundations.

Rogério Mascarenhas Silva (Secretary of Digital Government, Brazil)

Rogério Mascarenhas Silva serves as Brazil's Secretary of Digital Government within the Ministry of Management and Innovation in Public Services, where he leads the federal government's digital transformation and the expansion of inclusive, high-impact e-services. He brings over two decades of experience in public administration and digital policy, having previously directed large-scale modernization projects in state-level government before his appointment in 2023. Under his stewardship, Brazil has accelerated the rollout of GOV.BR services and strengthened digital access across urban and rural communities alike. He is particularly focused on safeguarding the digital government services infrastructure—a critical backbone for delivering healthcare, social welfare, and taxation systems efficiently and

equitably. In the Brazilian context, these digital platforms are lifelines that foster public trust, enable swift economic recovery, and ensure social inclusion across diverse regions. Rogério leads with calm confidence, valuing transparency and collaboration with civil society, local officials, and tech innovators in shaping responsive digital policy. Beyond his leadership in government, he is known for his quiet sense of humor and empathetic approach to both colleagues and citizens. In his leisure time, he enjoys restoring vintage vinyl records, an analog escape that contrasts with his digital day-to-day, and boarding long-distance cycling tours through Brazil's coastal towns, reminding him of the human connections behind every line of code.

John Doyle (CTO for Healthcare & Life Sciences, Microsoft)

John Doyle serves as Microsoft's Chief Technology Officer for Healthcare, where he leads the company's global strategy to integrate cloud, AI, and cybersecurity solutions into the health sector. With more than two decades of experience in healthcare IT and digital transformation, he previously directed modernization projects in clinical data systems and enterprise platforms before joining Microsoft. At the company, he has driven the expansion of the Cloud for Healthcare initiative, advanced AI-assisted clinical workflows, and strengthened cybersecurity protections for hospitals, insurers, and life sciences organizations. John places particular emphasis on reinforcing the resilience of healthcare infrastructure, recognizing that electronic health records, telemedicine platforms, and supply chain systems are essential to public health security. He views healthcare technology as a lifeline, one that must remain reliable to preserve patient trust and ensure continuity of care. Known for his collaborative leadership, he works closely with providers, policymakers, and innovators to design solutions that are both

technologically advanced and ethically grounded. Beyond his professional responsibilities, John is admired for his approachable demeanor and his commitment to mentoring future leaders in the health IT community. In his free time, he enjoys long-distance running and exploring culinary traditions with his family—reminders of the human connections at the heart of every technological system.

Anika Deshmukh (CTO for Finance, Microsoft)

Anika Deshmukh is Microsoft's Chief Technology Officer for Finance, directing the company's efforts to strengthen the digital backbone of global markets. With more than two decades of experience in financial engineering and enterprise technology, she has led the design of high-frequency trading systems, digital payment networks, and enterprise-scale compliance platforms. At Microsoft, her mandate includes scaling the Cloud for Financial Services platform, integrating AI into risk modeling and regulatory reporting, and advancing quantum-safe encryption for banking and capital markets. She views the financial sector not only as an engine of economic growth but also as a critical system whose stability underpins public trust and political security. Known for her precision and decisiveness, she works closely with central banks, regulators, and market operators to align technological innovation with systemic safeguards. Her leadership is defined by pragmatism and a clear focus on stability, ensuring that new solutions strengthen rather than strain the resilience of financial infrastructure. Beyond her professional role, Anika is recognized for her rigorous approach and her ability to mentor rising leaders in the fintech space. In her free time, she enjoys cycling long distances and reading economic history, finding in both a reminder that resilience and endurance are as vital to people as they are to markets.

Daniel Williams (CTO for Aviation, Microsoft)

Daniel Williams serves as Microsoft's Chief Technology Officer for Aviation, where he leads the company's strategy to bring cloud, AI, and digital twin technologies into global aviation systems. He has over twenty years of experience in aerospace engineering and aviation technology, having previously overseen modernization projects in air traffic management, predictive maintenance, and flight operations before joining Microsoft. At the company, he has advanced the use of AI for real-time route optimization, expanded digital twin platforms for aircraft and airport infrastructure, and strengthened cybersecurity for critical aviation networks. Daniel is particularly focused on enhancing the safety and reliability of global air travel. He believes that innovations in aviation technology must not only improve efficiency but also safeguard passengers, crews, and supply chains that depend on uninterrupted air mobility. Known for his strategic vision, he partners with airlines, regulators, and airport authorities to align cutting-edge technology with stringent safety and operational standards. Beyond his professional role, Daniel is recognized for his problem-solving mindset and his commitment to mentoring engineers transitioning into aviation technology. In his personal life, he is an avid pilot and enjoys hiking in remote regions, finding inspiration in both the complexity of the skies and the simplicity of the natural world.

Amir Rahman (CTO for Cloud Security, Microsoft)

Amir Rahman serves as Microsoft's Chief Technology Officer for Cloud Security, where he leads the company's global strategy to protect digital ecosystems against evolving cyber threats. With more than twenty years of experience in cybersecurity and enterprise technology, he has built his career around safeguarding critical infrastructure and securing large-scale cloud

environments. Before joining Microsoft, he directed threat intelligence and incident response programs for Fortune 100 companies, developing frameworks that are now industry benchmarks. At Microsoft, he has spearheaded advances in zero-trust architectures, pioneered the integration of AI in real-time threat detection, and strengthened encryption and identity management solutions that serve enterprises and governments worldwide. Amir sees cloud security as the foundation of digital trust in an interconnected world. He emphasizes that the reliability of finance, healthcare, energy, and public services depends on the resilience of cloud platforms. Known for his decisive leadership, he collaborates with policymakers, security researchers, and industry coalitions to shape standards that anticipate tomorrow's risks. His approach balances rapid innovation with a deep commitment to ethical responsibility and user protection. Outside of his professional role, Amir is recognized for mentoring the next generation of cybersecurity professionals. In his free time, he enjoys mountaineering and playing classical guitar, finding both pursuits a reminder of discipline, focus, and balance.

Elena Markovic (CTO for Trade, Microsoft)

Elena Markovic serves as Microsoft's Chief Technology Officer for Trade, where she leads efforts to modernize global commerce through cloud, AI, and blockchain-enabled solutions. With more than twenty years of experience in logistics technology and digital supply chain transformation, she previously managed large-scale modernization projects for customs authorities, shipping firms, and global trade networks before joining Microsoft. At the company, she has advanced the use of AI for real-time trade compliance, expanded blockchain pilots for secure cross-border transactions, and enhanced digital platforms that connect exporters, importers, and regulators. Elena views trade as the circulatory system of the global

economy—vital to growth, stability, and resilience. She is particularly focused on reducing friction in cross-border movement, ensuring that digital trade systems remain transparent, secure, and interoperable across jurisdictions. Known for her pragmatic leadership, she works closely with governments, multinational corporations, and logistics providers to design solutions that improve efficiency while upholding international standards. Beyond her professional role, Elena is recognized for mentoring women in technology and global logistics, helping diversify leadership in an industry still undergoing digital transition. In her personal life, she enjoys sailing and studying culinary traditions from port cities around the world, drawing inspiration from the interconnectedness of global trade.

BIBLIOGRAPHY

Advisory Board. “How Health Systems Responded to the CrowdStrike Outage.” *Advisory Board*, July 22, 2024. https://www.advisory.com/daily-briefing/2024/07/22/crowd-strike.

Border Crossing into US. 2007. *Flickr*, Peace Bridge, Buffalo, NY, https://www.flickr.com/photos/chapstickaddict/973379513.

Becker’s Hospital Review. “‘Worse than a Cyberattack’: 10 Notes on the Microsoft–CrowdStrike IT Outage.” *Becker’s Hospital Review*, July 22, 2024. https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/worse-than-a-cyberattack-10-notes-on-the-microsoft-crowdstrike-it-outage/.

Benoist, Jean-Christophe. NYC - New York Stock Exchange. 2012. Wikimedia Commons.

Bloomberg. “Microsoft Cloud Service Issues Disrupt Air Travel, Operations.” *Bloomberg*, July 19, 2024. https://www.bloomberg.com/news/articles/2024-07-19/microsoft-cloud-service-issues-disrupt-air-travel-operations?embedded-checkout=true.

Bloomberg. “CrowdStrike Earnings Beat Estimates in First Report after Cuts.” *Bloomberg*, June 3, 2025. https://www.bloomberg.com/news/articles/2025-06-03/crowdstrike-earnings-beats-estimates-in-first-report-after-cuts?embedded-checkout=true.

Burga, Solcyré. “Here Are the States Is 911 Impacted Due to the Tech Outage.” *Time*, Time, 19 July 2024, time.com/7000621/911-impacted-microsoft-outage/.

CIO Dive, “CrowdStrike Disruption Direct Losses to Reach $5.4 B for Fortune 500, Study Finds,” *CIO Dive*, July 25, 2024, accessed August 11, 2025, https://www.ciodive.com/news/crowdstrike-cost-fortune-500-losses-cyber-insurance/722463/.

CNBC, “Here Are the Top 15 Busiest Airports in the World,” *CNBC*, July 8, 2025, accessed August 11, 2025, https://www.cnbc.com/2025/07/08/here-are-the-top-15-busiest-airports-in-the-world.html#:~:text=Hartsfield%2DJackson%20Atlanta%20International%20Airport,billion%20people%20traveling%20by%20air.

CrowdStrike, “CrowdStrike Investors Double Down and Lead $100 Million Series D Round to Support the Company’s Global Growth,” *CrowdStrike Blog*, May 16, 2017, https://www.crowdstrike.com/en-us/blog/crowdstrike-investors-double-down-and-lead-100-million-series-d-round-to-support-the-companys-global-growth/.

Cybersecurity and Infrastructure Security Agency (CISA), “The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years,” *CISA News & Events*, May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

Dean, Grace. “Commuters in NYC and DC Should Get Ready for a Difficult, Disrupted Journey Due to the Global It Outage.” *Business Insider*, Business Insider, www.businessinsider.com/nyc-dc-subway-global-it-outage-crowdstrike-new-york-washington-2024-7. Accessed 16 June 2025.

Dexon Systems. “Redundant Systems: Definition, Types, and Use Cases.” Accessed August 14, 2025. https://dexonsystems.com/blog/redundant-systems.

D’Innocenzio, Anne, and Haleluya Hadero. “Many Small Businesses Struggle to Resume Normal Operations Days after Global Tech Outage.” *PBS*, Public Broadcasting Service, 21 July 2024, www.pbs.org/newshour/economy/many-small-businesses-struggle-to-resume-normal-operations-days-after-global-tech-outage.

EAS Barcelona, “How Many Planes Fly per Day Around the World,” *EAS Barcelona*, accessed August 11, 2025, https://easbcn.com/en/how-many-planes-fly-per-day-around-the-world/#:~:text=Global%20air%20traffic%20is%20one%20of%20the,100%2C000%20and%20130%2C000%20flights%20per%20day%20worldwid.

Economic Times. “Banks in India Affected by Global Microsoft Outage.” *The Economic Times*, July 19, 2024. https://economictimes.indiatimes.com/tech/technology/microsoft-outage.

Encyclopaedia Britannica, “Microsoft Corporation,” *Encyclopaedia Britannica*, last modified June 14, 2024, https://www.britannica.com/money/Microsoft-Corporation.

ePlaneAI, “The Impact of AI on the Aviation Cloud Market,” *ePlaneAI*, June 9, 2025 (accessed via supplemental summary).

Fortinet. “What Is Endpoint Security?” Accessed August 14, 2025. https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security#:~:text=End

point%20security%20is%20the%20process,malware%20being%20installed%20on%20endpoints.

Investor's Business Daily. "CrowdStrike Stock Falls amid Cybersecurity, Corporate Crisis Response." *Investor's Business Daily*, July 22, 2024. https://www.investors.com/news/technology/crowdstrike-stock-crwd-cybersecurity-corporate-crisis-management/.

Lori Ann LaRocco. "Microsoft, Crowdstrike It Outage Hits Global Supply Chain, with Air Freight Facing Days or Weeks to Recover." *CNBC*, CNBC, 19 July 2024, www.cnbc.com/2024/07/19/crowdstrike-it-outage-spreads-global-supply-chain.html.

Microsoft It Outage: Border Crossings into the U.S. Delayed by the Internet Disruption, nationalpost.com/news/world/microsoft-it-outage-updates. Accessed 17 June 2025.

Microsoft Köln, RheinauArtOffice, Rheinauhafen Köln. 2023. *FedScoop*. https://fedscoop.com/microsoft-launches-azure-openai-service-for-government/.

Microsoft, "Microsoft Shares Strong Progress on Datacenter Region in Saudi Arabia; Construction Complete on Three Sites, with Availability Expected in 2026," *Microsoft News*, December 4, 2024, https://news.microsoft.com/en-xm/2024/12/04/microsoft-shares-strong-progress-on-datacenter-region-in-saudi-arabia-construction-complete-on-three-sites-with-availability-expected-in-2026/.

"Microsoft Outages Affecting Dispatch Centers across the Country." *FireRescue1*, FireRescue1, 19 July 2024,

www.firerescue1.com/911-and-dispatch/microsoft-outages-affecting-dispatch-centers-across-the-country.

New York Post. “Flight Troubles Linger Following Global Tech Outage; Hospitals, Businesses Work to Get Back on Track.” *New York Post*, July 20, 2024. https://nypost.com/2024/07/20/world-news/flight-troubles-linger-following-global-tech-outage-hospitals-businesses-work-to-get-back-on-track/.

Organisation for Economic Co-operation and Development (OECD), *Competition in the Provision of Cloud Computing Services*, OECD Roundtables on Competition Policy Papers No. 3 (2025), Paris: OECD Publishing, https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf.

StatCounter Global Stats, “Desktop Operating System Market Share Worldwide,” accessed August 11, 2025, https://gs.statcounter.com/os-market-share/desktop/worldwide.

Pharmacy Times. “CrowdStrike Reports Global Outage Affecting Hospitals, Businesses across the World.” *Pharmacy Times*, July 20, 2024. https://www.pharmacytimes.com/view/crowdstrike-reports-global-outage-affecting-hospitals-businesses-across-the-world.

Reuters. “CrowdStrike Deploys Fix for Issue Causing Global Tech Outage.” *Reuters*, July 19, 2024. https://www.reuters.com/technology/crowdstrike-says-actively-working-with-customers-impacted-by-outage-2024-07-19/

Reuters. “CrowdStrike Update That Caused Global Outage Likely Skipped Checks, Experts Say.” *Reuters*, July 20, 2024. https://www.reuters.com/technology/cybersecurity/crowdstrike-update-that-caused-global-outage-likely-skipped-checks-experts-say-2024-07-20/.

Reuters. “Global Tech Outage Creates Challenges for Canadian Health Infrastructure.” *Reuters*, July 19, 2024. https://www.reuters.com/technology/global-tech-outage-creates-challenges-canadian-health-infrastructure-2024-07-19/.

Reuters. “Global Tech Outage Delays Flights, Disrupts Services around World.” *Reuters*, July 19, 2024. https://www.reuters.com/business/aerospace-defense/global-tech-outage-delays-flights-disrupts-services-around-world-2024-07-19/.

Reuters. “JPMorgan Says Majority ATMs Operating Normally amid Outages.” *Reuters*, July 19, 2024. https://www.reuters.com/business/finance/jpmorgan-says-majority-atms-operating-normally-amid-outages-2024-07-19/.

Reuters. “LSEG’s Workspace Platform Suffers Outage, Market Sources Say.” *Reuters*, July 19, 2024. https://www.reuters.com/technology/lsegs-workspace-platform-suffers-outage-market-sources-say-2024-07-19/.

Reuters. “Microsoft Says about 8.5 Million of Its Devices Affected by CrowdStrike-Related Outage.” *Reuters*, July 20, 2024.

https://www.reuters.com/technology/microsoft-says-about-85-million-its-devices-affected-by-crowdstrike-related-2024-07-20/.

Reuters. “Traders in London and Singapore Struggle as Cyber Outage Disrupts Business.” *Reuters*, July 19, 2024. https://www.reuters.com/technology/traders-london-singapore-struggle-cyber-outage-disrupts-business-2024-07-19/.

Reuters. “Two German Hospitals Cancel Elective Operations, Citing Global IT Outage.” *Reuters*, July 19, 2024. https://www.reuters.com/business/healthcare-pharmaceuticals/two-german-hospitals-cancel-elective-operations-citing-global-it-outage-2024-07-19/.

Reuters. “What Disruptions Have Been Reported after Global Tech Outage?” *Reuters*, July 19, 2024. https://www.reuters.com/markets/commodities/what-disruptions-have-been-reported-after-global-tech-outage-2024-07-19/.

Smishra1. CrowdStrike BSOD at LGA. July 19, 2024. Wikimedia Commons. https://upload.wikimedia.org/wikipedia/commons/9/94/CrowdStrike_BSOD_at_LGA.jpg.

TechTarget. “What Is Canary Testing?” *TechTarget*, August 31, 2022. Published by Rahul Awati and Peter Loshin. https://www.techtarget.com/whatis/definition/canary-canary-testing

Tesla Halted Some Production Lines Due to Global It Outage, Business Insider Reports | *Reuters*,

www.reuters.com/business/autos-transportation/tesla-halted-some-production-lines-due-global-it-outage-business-insider-reports-2024-07-19/. Accessed 16 June 2025.

Venture in Security, "20 Years of Cybersecurity Consolidation: How 200 Companies Became 11," *Venture in Security* (Substack), August 5, 2025, https://ventureinsecurity.net/p/20-years-of-cybersecurity-consolidation.

Wired. "Hospitals Were Hit Hard in CrowdStrike–Microsoft IT Outage Meltdown." *Wired*, July 22, 2024. https://www.wired.com/story/hospitals-crowdstrike-microsoft-it-outage-meltdown/.

www.ETManufacturing.in. "Microsoft Outage: How the Global Outage Affected the Manufacturing Industry? Uncovers Cloud Dependency Risks - et Manufacturing." *ETManufacturing.In*, 20 July 2024, manufacturing.economictimes.indiatimes.com/news/industry/microsoft-outage-how-the-global-outage-affected-the-manufacturing-industry-uncovers-cloud-dependency-risks/111881325#:~:text=Many%20manufacturing%20companies%20rely%20on,risk%20of%20mistakes%20and%20inefficiencies.