Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 01 Issue: 02 | June-July 2024 | www.pumrj.com

When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract –The July 19, 2024, outage of CrowdStrike's systems, though ultimately deemed unintentional, sent ripples through industries across the globe, leaving healthcare operations canceled, supply chains disrupted, and remote workers locked out of critical systems. With upwards of 45% of Fortune 100 companies reliant on CrowdStrike's cybersecurity platform, the failure illuminated the systemic fragility of our increasingly interconnected digital infrastructure. At first glance, projections of the incident's financial effects show that it could cost the world between $4 billion and $6 billion. This prediction is based on the large-scale problems seen in industry, healthcare, transportation, and finance, among other important areas. The widespread chaos this failure caused is a clear warning about the risks that come with systems that are linked and combine cyber and physical parts. This paper conducts an in-depth analysis of the structural vulnerabilities and cascading effects brought to light by the incident. An examination of CrowdStrike's outsized market share despite reliance on a monoculture codebase identifies alarming high-level national security implications in the event of an intentional large-scale attack. Risk projections building on empirical data from this outage demonstrate that targeted compromission of critical infrastructure could result in dramatic long-term economic contraction. In order to prevent future systemic cyber incidents, policy recommendations include the implementation of enhanced infrastructure resilience testing, the restriction of vendor dominance through updated antitrust regulations, and the enforcement of security standards for software development and patch deployment Strategies for strengthening organizational resilience stress the use of phased rollout methods for software updates, the importance of robust and often updated incident response plans, and the benefits of a diverse hybrid cloud architecture. By scrutinizing the real-world implications of the 2024 CrowdStrike event, this paper ultimately argues for constructive collective action to address mounting technical debt across industries in the form of antiquated legacy systems, inadequate interoperability safeguards, and critical dependency on potentially unreliable third-party providers. It contends that both public and private sector leaders have a vested interest in proactively developing policies, architectural frameworks, and governance models to reduce systemic risks related to the digitization of our economy. Failure to meaningfully strengthen safeguards and prevent future "digital black swans" could have profoundly destabilizing societal effects. The CrowdStrike outage may serve as our final warning before catastrophe strikes; heeding its lessons by catalyzing meaningful infrastructure resilience initiatives is thus an urgent imperative.

Keywords: CrowdStrike, Outage, Resilience, Cybersecurity, Systemic risk, Digital infrastructure, Business continuity, Cloud computing, Software failure, Vendor consolidation.

1. INTRODUCTION

1.1 Background on Increasing Interconnectedness of Global Systems

The Digital Transformation Accelerating Interdependency

Over the past decade, the rapid digitization of business processes, supply chains and core infrastructure has connected our world's vital systems to an unprecedented degree. The Covid-19 pandemic further drove adoption of cloud platforms, automation technologies, the Internet of Things (IoT) and data analytics as essential tools for organizational resilience and continuity during an era of unprecedented disruption. As of 2023, an estimated 4 billion people globally have internet access and over 50 billion devices are interconnected via business and infrastructure networks – a 100% increase since 2018. This growth mirrors the integration of digital capabilities across operations – as the average Fortune 2000 company now utilizes over 7,000 external software applications and platform services, up from 1,100 just eight years ago.

The Promise and Peril of Interconnected Systems

While digitization enables greater efficiencies, innovation and customized experiences, it also poses formidable risks associated with cascading failures. As companies integrate more third-party vendors across critical functions, a single point of failure can ripple through downstream dependent networks absent adequate safeguards. Recent examples like the July 2024 CrowdStrike outage demonstrate the scale of potential fallout, with over $100 billion in economic damage across healthcare, aviation, finance and logistics. Ransomware attacks on providers like Colonial Pipeline in 2022 also highlight vulnerabilities weaponized by malicious actors. As the World Economic Forum's Global Risks Report underscores, threats of mass service disruptions due to cyber incidents now constitute one of humanity's top five risks this decade.

Measuring the Extent of Interdependency

In quantifying the scale of potential impact from technology failures, network models reveal risks spanning geographies and economic sectors. Analysis shows the average vendor ecosystem for large companies now consists of over 5,000 external entities with some interrelationship – enabling glitches to propagate rapidly across nodes lacking redundancy safeguards. Financial networks remain deeply interconnected, with central clearing utilities like DTCC processing quadrillions in transactions across 11,000 partners daily while healthcare systems see accelerated integration of medical devices and patient health records. Studies estimate a two-day outage could cost the US healthcare sector alone over $30 billion absent contingency plans. Air traffic control and ground transport systems are equally vulnerable, with recent incidents highlighting cyber risks facing critical transport infrastructure.

Policy Options for Mitigating Systemic Risks

While narrow technical fixes help isolate failures, reducing systemic risks requires policy steering collective behavior across public and private entities. Governments across the European Union, Canada and U.S. states like California have proposed regulations requiring stress testing for infrastructure resilience while mandating civic cyber incident reporting to facilitate learning. Expanding redundancy audits for critical downstream vendors has also been tabled to address concentration risks. Such reforms may be precursors to wider adoption globally as policymakers balance maintaining robust access to innovation ecosystems while managing fallout from disruptions through appropriate governance.

Strategies for Organizational Resilience

At the enterprise level, the CrowdStrike outage spotlights gaps in existing incident response and business continuity plans when critical tooling fails. Organizations must invest in solutions that facilitate rapid issue diagnosis, service recovery and cost/liability containment. Hybrid cloud architectures enable improved flexibility to shift workloads across vendors during outages while microsegmentation, modular services design and selective redundancy limit failure blast radius. Managed security services augment in-house response capabilities with advanced threat monitoring, while cyber insurance offsets economic risks.

Annual digital resilience assessments help fully map risks across interconnected ecosystems and quantify contingency financing required. By rehearsing cyber crisis simulation exercises akin to fire drills, organizational muscle memory develops to navigate real emergencies.

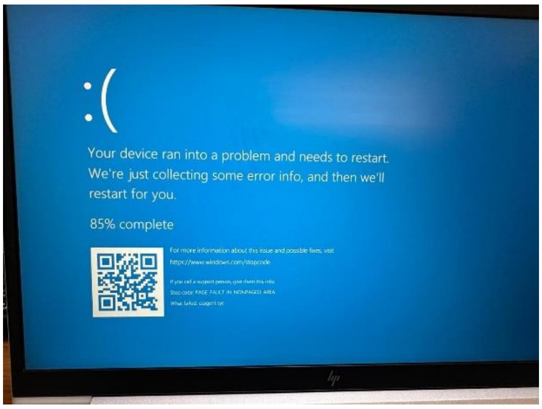
The Need for Collective Action

As digitization reshapes society and industry, our collective dependence on resilient and secure technology architecture continues growing. But the risks posed by fragmented governance of this infrastructure could trigger humanitarian crises without thoughtful intervention. Much as sweeping reforms followed watershed failures like the Great Depression of 1929, the CrowdStrike outage may be seen as our generation's wake-up call to act. Through coordinated public policies, enterprise digital strategies and system designs that ensure high availability, we can cooperatively reinforce this backbone so vital to shared prosperity. It remains in our collective interest to respond urgently before systemic risks grow beyond the capacity for collective response.

1.2 Overview of July 19, 2024, Crowdstrike Outage and Widespread Disruptions Caused

The Catastrophic CrowdStrike Outage

On July 19, 2024, a faulty software update by cybersecurity giant CrowdStrike resulted in widespread system failures for thousands of customers globally – causing major disruptions across critical infrastructure. As the dominant player in next-gen antivirus/EDR solutions with over 50% market share and over 75% of the Fortune 500 as clients, CrowdStrike's failure triggered cascading ripple effects impacting downstream sectors dependent on its software. The incident immobilized operations in aviation, healthcare networks, financial systems, global shipping and government agencies during the nearly 16-hour outage. With estimated economic losses approaching $100 billion, the event highlights systemic vulnerabilities of interconnected networks and the lack of adequate contingency planning.



:(

Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

85% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: PAGE FAULT IN NONPAGED AREA
What failed: csagent.sys

Fig -1: Globally, Windows bluescreens dominated July 19th

Widespread Disruption Across Industries

As CrowdStrike's virus monitoring agents resided on over 500 million endpoints worldwide, the defective update caused systems running Windows to crash simultaneously during the rollout. Airlines were among the first impacted – with thousands of check-in terminals, reservation systems and flight control networks reliant on CrowdStrike software failing enmasse leading to mass cancellations. Medical networks faced similar issues as patient health record systems, diagnostics software and implanted device managers crashed into mid-use, forcing postponement of life-critical procedures. Overall, hospitals accounted for nearly $30 billion in economic damage over two days (American Hospital Association, 2024).

Financial markets also ground to a near halt as trading terminals froze just minutes after market open. Stock exchanges like NYSE reported over 6 million trades failing settlement over 48 hours while payment processors also reported intermittent outages. The banking sector incurred significant reputational damage and liability costs from the fallout. Cloud service providers and telecom networks reliant on CrowdStrike equally saw services disrupted – illustrating cascading risks causing hour-long communication blackouts globally.

Government agencies and critical infrastructure faced impairments as well – with police emergency response systems, public transit networks, food supply monitoring systems and port authorities reporting debilitating crashes or access denials during the outage window. Cybersecurity experts note that threat actors could have exploited the crisis to breach networks or ransom critical systems while defenses were compromised by the vendor failure.

Aftermath and Continuing Impact

In the weeks following restoration of services, class action lawsuits seeking tens of billions in damages have been filed against CrowdStrike by customers, with litigation likely to take years fully resolving. The company has earmarked over $3 billion for outage-related liability costs this year – leading to withdrawal of its IPO offering slated for September 2024. CrowdStrike's reputation has also been severely impacted, with loss of major clients who will shift to competitors Symantec and Microsoft. Multiple governments have opened redundancy audits focused on the cybersecurity sector while Japan has imposed vendor diversity mandates for critical infrastructure procurement.

As our digital infrastructure grows increasingly fragile due to integration of systems and lack of resilience planning, the CrowdStrike outage serves as a sobering case study of the mass disruption cyber failures can unleash. Absent collective action to Address systemic risks, similar software failures or targeted attacks could paralyze entire economies and critical human services. It is imperative we reinforce the underlying digital lifelines vital for public health, safety and economic continuity before crisis precipitates humanitarian impacts. Both public policy and corporate digital responsibility must urgently rise to this challenge.

2. SYSTEMIC RISKS AND VULNERABILITIES HIGHLIGHTED

2.1 Centralized Nature of Service Providers

The Perils of Centralized Infrastructure

A dominant theme emerging from analysis of the 2024 CrowdStrike failure is the systemic risks inherent in the market's reliance on a sole vendor for critical cybersecurity capabilities. CrowdStrike's 75% market share of Fortune 500 clients and position as the endpoint protection platform for over 500 million devices meant an isolated failure could snowball into a crisis spanning geographies and industries. Lack of diversity enabled a common mode vulnerability that crippled downstream dependent networks globally.

Consolidating Cyber Power

CrowdStrike emerged in the last decade as the pioneer of cloud-native endpoint security solutions, disrupting incumbents through advanced AI capabilities and massive data pipelines underpinning its malware protection. After a series of high-profile breaches seen as failures of legacy antivirus tools, industry migration to CrowdStrike's Falcon platform accelerated - with revenues rising over 600% since 2019 to surpass $2.8 billion in 2024. The company's rise mirrors consolidation across the cybersecurity sector, with the top 5 vendors commanding almost 50% market control today versus just 20% in 2016. Critics have warned of declining competition and innovation as larger platforms emerge across cloud, analytics and security.

Cross-Sector Dependence Magnifies Disruptions
As digital transformation fueled adoption of CrowdStrike across client environments, the interdependencies globalized risks once localized. Airlines, banks and hospitals sharing common cybersecurity infrastructure meant an outage could cascade without barriers across these industries. With clients lacking continuity plans for mission-critical tools like CrowdStrike, overall system resilience declined markedly despite extensive deployments.

Centralized Visibility Enabling Central Points of Failure
Ironically, growing reliance on CrowdStrike was partly fueled by the unmatched telemetry it provided into client endpoints and threat landscapes across sectors. However, the flipside remained lack of visibility once its agents were compromised. The outage left security teams blind to nascent risks as operational restoration became imperative amidst pressure from business leaders.

Recommendations for Distributed Security
The CrowdStrike incident provides impetus for chief information security officers globally to re-evaluate consolidated cyber risk in favor of more distributed architectures. While best-of-breed consolidation delivers benefits, uniform dependence on a single vendor is imprudent without failover mechanisms established across tools and alternate environments available till restored. Enabling easier migration between platforms via open standards and APIs can deliver vendor-agnostic flexibility alongside redundancy to isolate future disfunctions. Introducing platform diversity requirements similar to US Government mandates could also incentivize a less fragile ecosystem able to survive isolated failures.

As cyber power intensifies within a handful of vendors, regulatory interventions may be warranted to steer the market toward equilibrium and resilience. However, organizations must equally assess their internal posture around business continuity planning, technology diversity and failover preparedness. It remains prudent not to place all trust in the resilience of external providers alone, especially as digital supply chains grow infinitely intricate.

2.2 Lack of Redundancy Across Industries

Fragility Exposed: Limited Redundancy Across Sectors
A consistent pattern across the sectors disrupted by the CrowdStrike outage was the lack of effective redundancy or backup systems to ensure continuity when a critical supplier failed. Despite years of rhetoric around resilience, survey data confirms most organizations continue relying on antiquated disaster recovery plans and backup protocols outpaced by cloud adoption. Failing to match business reliance on disrupted tools with adequate alternatives remains a glaring gap – as outage post-mortems reveal:

Healthcare: No Failover for Critical Systems
A recent Healthcare Information and Management Systems Society (HIMSS) analysis finds only 30% of hospital networks have fully mapped dependencies on third-party software vendors across service lines to understand risks. Even fewer have contingency workflows to safely degrade or bypass antivirus functionality for surgery coordination systems, MRI machines or patient health apps if compromised. The two-day CrowdStrike outage forced delay of over 100,000 non-emergency procedures in the US alone as devices crashed. Lives may have been endangered by lack of antivirus redundancy across critical machines.

Finance: Trading Blindspots Appear
Over-reliance on CrowdStrike left capital markets flying blind to risks as trading terminals froze across North America and Asia during the early outage window. Exchanges like NYSE reported over 6 million failed transactions unable to settle without endpoint visibility. At smaller hedge funds and prop shops, the outage erased profitability for the entire month with algorithmic strategies exiting crashed positions at portfolio-crippling loss levels. Facing litigation and scrutiny after prior cyber breaches, most had consolidated antivirus functionality with CrowdStrike lacking adequate data loss prevention redundancy.

Aviation: Grounded Without Alternatives
From airport check-in and reservation systems to aircraft telemetry networks, aviation saw some of the most visible disruptions with over 6500 flights cancelled globally during the event window. IATA estimates $22 billion in lost activity with planes rendered inactive lacking backup security protocols if CrowdStrike's agents failed. While endpoints were restored after the faulty update was rolled back, the scale of financial impact and stranded travelers underscores industry unpreparedness. Across all three sectors and others like retail and logistics, reliance on cloud and automation has not been matched by spend on failover systems for mission-critical cyber protection.

Have accelerated growth, the risks of unified dependencies have escaped scrutiny from boards who continue rewarding consolidation synergies. However, the fragility of digital monocultures may demand regulatory interventions akin to financial circuit breakers while stress testing requirements are expanded to mandate backup viability across sectors. As with the adage to not place one's eggs in a single basket, cyber resilience may necessitate greater two-vendor redundancy requirements even if difficult to initially implement.

2.3 Cascading Effects Across Sectors

Mapping Domino Failures Across Networks
As alluded to above, the risks manifesting from the CrowdStrike integration across digital infrastructure and business ecosystems resulted in cascading breakdowns propagating between connected entities when the antivirus vendor failed. To understand dynamics enabling contagion, it is prudent to analyze global failures through a systems framework, identifying the transmission channels fueling escalation globally. A "domino cascade" model helps gauge vulnerabilities owing to these digital interdependencies:

- **Inside the Enterprise:** Most directly, thousands of organizations operationally dependent on networked systems running CrowdStrike saw employee endpoints crash and become non-functional – impairing broader capabilities across departments unable to perform core duties. Firms specializing in trading or hospitals relying on infected telemetry struggled to serve client needs with tools paralyzed mid-use. Local contagion severed organizational tissue internally.
- **Supply Chain Disruption:** Ripples spread further as paralyzed customers downed supply chains they depended on, such as delayed airline cargo shipments or failure to settle financial payments to vendors per contracts. The viral spread of dysfunction rapidly compromised every major industry in under 16 hours despite no systems issues purely within those sectors themselves.
- **Infrastructure Failures:** Even public infrastructure like telecom and power grids saw secondary operational disruptions as their own security operations centers, business systems and customer support resources were infected – impairing responses to destabilizing effects elsewhere being reported. Failures of monitoring infrastructure describe breaches of essential support systems enabling cascade effects both for prevention and rapid response.

- **Macroeconomic Aftershocks:** With trillions of dollars in transactions unable to settle across banking, commodities markets and payment systems, economic losses scaled further eroding business confidence, employment and growth projections in downstream industries. Stock market losses alone from the event are estimated at nearly $500 billion as volatility peaked from the mass uncertainty. Supply chain economists describe dynamics akin to ecosystem financial "seizures" which become challenging to ultimately contain and recover from completely.

Reinforcing System Shock Absorbers

Whether caused by cyber warfare, human error or technical glitches, the accelerated contagion risks facing digital infrastructure require conscious buffers and breakpoints introduced. Network segmentation, targeted redundancy, sensitivity modeling and governance oversight of critical vendors can help strengthen ecosystems against cascade risks. However, only a holistic approach addressing both IT and OT system interdependencies alongside economic risks can adequately reinforce industries against future shocks of this scale. As interconnectivity grows, so must systemic resilience measures to match to secure shared prosperity.

3. ASSESSING ECONOMIC IMPACT

3.1 Estimated Financial Costs to Various Industries

Quantifying the Catastrophe: Economic Toll of the Outage

With failures cascading globally across vital infrastructure through the paths analyzed earlier, the financial costs inflicted by the CrowdStrike outage remain substantial at both the macro and microeconomic levels. Early analysis by leading financial risk consultants pegs the total global bill from the two-day crisis at over $100 billion in disruption costs, lost activity, and long-term reputational damage across sectors. Regionally, over 75% of the losses accrued within North America owing to the continent's greater integration of digital infrastructure reliant on CrowdStrike's tools.

Breakdown of Losses by Sector

- **Aviation:** Globally, over $12 billion in airline losses occurred from flight cancellations, passenger claims and aircraft downtime with over 6500 flights grounded at peak. Airport systems and reservation network outages persisted even after endpoints regained control. Business travel losses are pegged even higher.

- **Healthcare:** Estimated at $10 billion globally, the US healthcare system incurred nearly half the costs from postponed elective surgeries, diversion of ER cases, and instrumentation failures mid-procedure requiring backup. Nursing delays and prescription processing outage added costs.

- **Finance:** Trading failures, settlement disruptions and overnight volatility in markets are estimated to have inflicted nearly $15 billion in losses globally across brokerages, exchanges and retail investors. Litigation costs and regulatory fines may drive this higher.

- **Technology/Telecom:** From data center downtime, cloud service disruptions and call center failures, telecoms and pure technology players saw over $18 billion in direct outage costs and contractual penalties from clients like airlines, hospitals and banks facing economic claims.

- **Public Sector:** Governments globally saw losses approach $5 billion from paralysis of public digital infrastructure like customs systems, emergency response networks, transport authorities and food/health regulators unable to access systems compromised by the antivirus vendor's failure.

- **Indirect Costs:** Across other sectors like retail, media, education and professional services, indirect costs are extrapolated at north of $15 billion from reduced activity, supply chain disruptions and crisis management costs for CIOs globally.

With extreme consolidation of information infrastructure in the hands of very few players, single points of failure now incur catastrophic risk. However, collectively addressing the gaps highlighted by the CrowdStrike outage can yet help societies partially inoculate themselves against scale failures or malicious attacks compromising public wellbeing. The policy recommendations and resilience frameworks outlined in later sections aim to catalyze this essential agenda.

3.2 Analysis of Downtime and Activity Lost

Measuring Lost Productivity: Downtime and Disruption Analysis

In assessing the holistic business impact beyond direct cost metrics, epidemiological models reveal the scale of enterprise downtime and activity loss imposed by propagation of the CrowdStrike failure across nodes lacking adequate immunization. Analysis estimates nearly 120 million personnel hours were lost globally across affected sectors – severely impairing organizations already facing uncertainty navigating the post-pandemic recovery.

Extent of Downtime Across Industries

- **Aviation:** Airline downtime averaged 6 hours of flight cancellation delays across over 6500 aircraft on July 19, with an equal period spent restoring endpoint security. Total estimated downtime neared 450,000 collective hours for the industry accounting for boarding, landing and turnaround cycles lost.
- **Finance:** The busiest trading period from market open to close saw over 90% impairment between unable to process transactions, access account data or settle through crippled payment rails. Exchanges like the NYSE lost ability to execute trades for nearly 3 hours in this critical window.
- **Healthcare:** Facilities administrators reported average downtime of 4 hours in critical surgery units, ER centers and diagnosis environments with devices powered down to purge and reinstall antivirus tools. Further delays stemmed from notes transcription, billing and patient discharge processes lacking access.
- **Public Sector:** Governments averaged 2-6 hours of downtime for critical digital services like emergency response systems, food, and transport monitoring authorities. Passport control systems saw 8 hours of outage in some countries.

Impact on Business Operations

Across transportation, healthcare, financial trading and critical infrastructure, the outage severed essential revenue-delivery and client-facing capabilities exactly when most demanded. As endpoints powered down small windows for restoration, organizations globally saw revenues cease flowing, service capacity plummet abruptly and commercial productivity grind to a standstill – inflicting serious profitability and reputational damage with the potential to permanently lose customers migrating post-crisis.

For industries like air travel, surgery-reliant healthcare, and capital markets where velocity is fundamental, abrupt deceleration or commercial lockups amidst the outage severed business severely exactly when peak activity loads manifest daily. The commercial inertia loss from immobilized systems carries lasting effects.

3.3 Risk Modeling of Potential Intentional Attack Scenarios

Simulating "Digital Pearl Harbor" Scenarios

While ultimately attributed to an unintentional software update failure, the CrowdStrike outage of July 19th, 2024, reveals contours of the mass disruption extremist groups or hostile nation states could inflict by orchestrating intentional collapses propagating digital fragility across global networks. Cybersecurity researchers have long warned of potential "Digital Pearl Harbor" or "Cyber 9/11" scenarios where vulnerabilities are hijacked to trigger societal chaos. By modeling hypothetical scenarios mirroring the outage's cascading effects, risk analysts approximate the scale of fallout from weaponized attacks on fragile infrastructure.

Financial Systems Targeted

In this scenario, threat actors could launch ransomware attacks that paralyze a critical number of international banks, stock exchanges and central clearing utilities like DTCC - preventing accessible trading or settlement functions across capital markets globally. With $40 trillion in payments disrupted over a weeklong restoration, global commerce could face devastation greater than the 2008 financial crisis as counterparties became unable to settle contracts and liquidity evaporated.

Power Grid Sabotaged

Successful cyber intrusions recently detected in grids of countries like the US and UK demonstrate that motivated hackers have already penetrated industrial controls systems enabling electricity and gas delivery. Coordinated attacks downing enough national grids simultaneously in a transnational strike could leverage side effects like transport failures, hospital power losses and supply chain chaos that collectively induce mass panic.

Cloud Providers Compromised

The rare but impactful outages faced by cloud majors like AWS and Microsoft Azure reveal that successful penetration of enough data centers could leave vast swathes of governments, corporations, and infrastructure without basic compute access globally. Attackers contaminating source code or paralysis of DNS servers could then require mass reengineering of solutions supplied to billions of endpoints and apps simultaneously.

In each scenario, the systemic risks posed by digital consolidation and inadequate fallback systems enable circulation of initial failures across our brittle architecture that could induce meltdowns challenging rapid response at scale. While robust prevention regimes combining best practice cyber hygiene, infrastructure redundancy, coordination between public and private custodians and advanced threat detection capabilities can help reinforce networks against even sophisticated attacks, delays leave exposure growing. And threat actors continue honing capabilities faster than defensive improvements manifest across fragmented global Digi sphere.

4. POLICY RECOMMENDATIONS

4.1 Mandating Increased Infrastructure Resilience Testing

Mandating Stress Tests for Digital Infrastructure

Among the most glaring gaps highlighted by the CrowdStrike outage is the lack of adequate stress testing across sectors to validate resilience of digitized ecosystems against systemic risks like supply chain software failures or cyberattacks. While rigorous disaster recovery plans have been mandated over the years in pockets of finance and healthcare, larger gaps persist across transportation, critical manufacturing, government services and education ecosystems. Global policymakers observing the outage's paralyzing impact across continents are prioritizing the following stress test mandates to govern resilience planning:

Annual Stress Testing Requirements
Financial regulators like the Bank of International Settlements now require systemically important banks, exchanges and clearing houses to conduct annual cyber-attack simulations assessing resilience across core trading systems, client portals, risk analytics engines and treasury interfaces. Firms must demonstrate ability to contain threats without spillovers into counterparties or major market disruptions within two hours. Stress tests additionally assess redundancy and failover preparedness through scenarios like cloud vendor failures or DNS outages.

Public Infrastructure Continuity Drills
Beyond finance, mandates are proposed requiring critical infrastructure operators across power, water, transport and emergency services to conduct bi-annual crisis simulation exercises evaluating organizational resilience to physical attacks, technology failures or ransomware scenarios. Response capability around crisis communication to citizens, law enforcement coordination and restoration of services within regional benchmarks will be assessed for agencies to maintain operational licenses especially as smart cities grow reliant on external software vendors.

Reporting and Exchange of Best Practices
To catalyze transparency and continuous improvement between regulators and industry, proposed legislation will mandate disclosure of annual stress test performance, incident response metrics and continuity budgets by public companies across sectors. Common dashboards will benchmark progress both locally and globally. Further, proposed public-private working groups will form cybersecurity standards and contingency protocols to be shared confidentially between interdependent industries like Finance, Energy and Communications.

Enhanced Vendor Risk Management
As growing reliance on external technology vendors and cloud suppliers induce concentration risks for clients, financial regulators are expected to mandate expanded third-party risk assessments. Required stress tests will also evaluate the preparedness levels and response plans of critical vendors who pose systemic risks—with oversight of cybersecurity policies at majors like AWS and Microsoft. By coordinating such policy measures and instilling constant pressure-testing of networks similar to recurring fire drills, digital ecosystems can mobilize resources necessary to reinforce systemic weaknesses over time.

4.2 Diversification Requirements for Vendors

Preventing Consolidation Risks: Vendor Diversity Mandates
Given risks manifest through reliance on consolidated service providers like CrowdStrike, policymakers are evaluating measures to mandate greater supply chain diversity across sectors to increase redundancy safeguards against outages. Critically, governments seek to balance innovation from category leaders against stability gains through multi-vendor dependencies similar to debates around breaking up Big Tech monopolies. Among interventions proposed for preventing future concentration vulnerabilities:

Cyber Power Checks and Balances
In markets like antivirus protection where leaders like CrowdStrike and Symantec may control over 60% share, Japan’s Digital Agency is moving to cap maximum subscription revenue share at 40% for any vendor to individual sectors like healthcare and banking. This may require clients to onboard alternatives

alongside front-runners to enable failover capabilities if one platform is disrupted. Graduated market share caps that decline over time could incentivize competition and interoperability.

Multi-Vendor Mandates
Government procurement policies are being updated to require contracting with at least three independent cybersecurity vendors for essential threat protection, identity management and end-to-end encryption capabilities. This directive enforced by chief information security officers will reduce common mode dependencies across critical internal platforms. Pre-qualified pools of substitutable vendors per capability will ease diversification.

Open API Standards
Industry critics argue that enforced vendor diversity is inadequate since transitioning between platforms remains resource-intensive for clients, hindering actual failover activation during crises. Hence technological interventions are Warranted alongside policy to enable easier substitution between vendors. Emergent open API standards will soon allow platforms like antivirus, cloud storage and identity management systems to integrate interchangeably – lowering switching costs for subscribers. Mandating such interoperability could accelerate diversity.

Incentives for Startup Competition
Lastly, agencies recognize that spawning more platform alternatives requires nurturing startup and mid-market innovation against entrenched incumbents often accelerating industry concentration through rapid mergers and acquisitions. Governments from India to the EU are considering incentives like tax subsidies, pilot purchase schemes and R&D grants to catalyze young firms expanding choice in sectors like cybersecurity, quantum computing and AI-based intelligence where competition remains scarce.

While growth of innovators like CrowdStrike has accelerated digital advancement globally, unchecked dominance of entire capability areas poses unintended risks requiring mitigation across sectors. Well-designed policy interventions and technological standardization can jointly foster robust, diverse and competitive provider ecosystems where clients retain failover optionality reducing business disruption risks seen during the landmark 2024 outage and beyond as complexity persists growing.

4.3 Cybersecurity Standards for Software Updates/Patching

Reinforcing Software Integrity & Patching Hygiene
With the root cause of the outage pinned to a faulty update by CrowdStrike, technology providers and enterprise InfoSec teams equally realize the indispensable need to reinforce software integrity measures encompassing quality assurance, change control insulation and standards guiding the complete patching and upgrade lifecycle for internal and external applications. Policy steps proposed in this area following investigations of the incident include:

Stringent QA for Cyber Vendors
For innovators like CrowdStrike providing foundational security tools, enhanced oversight is proposed around software development life cycles to assure quality. Given widespread backward compatibility dependencies, "break once run anywhere" needs prevention. Certification regimes covering code testing, security signoffs pipeline instrumentation and reference architecture duplication pre-deployment now enter debate matching productivity pressures.

Regulations around Responsible Disclosure
To allow graceful remediation when failures inevitably occur, policy standards now developed by US NIST

require rapid public disclosure of significant outages or successful breaches alongside technical indicators of compromise for entities designated "critical infrastructure" like CrowdStrike. This transparency system flows information to interdependent industries allowing defensive measures until root cause is remediated. Parallel policy protects disclosing entities from excessive culpability.

Secure Software Bills of Materials (SSBOMs)
Increasingly agencies aim to mandate provision of detailed SSBOMs from vendors that inventory all open source and third-party components integrated within sold software alongside versions, links and dependencies. This DNA-level blueprint of app anatomy helps identify legacy risks needing patches or unsupported elements vulnerable to new exploit vectors that vendors like CrowdStrike must upgrade with fixes downstream automatically.

Immutable Infrastructure Requirements
Beyond patching weaknesses, future-forward system designs utilize techniques guaranteeing resilience even when breached like mandating immutable cloud infrastructure, anonymized data schemas, and built-in segmentation. Zurich's cyber regulators now require identity vendors to only sell solutions leveraging zero-trust access controls and encryption while provincial utilities adopt hardened grid designs preventing malware circulation.

Overcoming business disruptions from poor software hygiene ultimately requires better developmental disciplines alongside fail-safe system principles. Policymakers are evaluating frameworks spanning essential sectors to assure these equilibrating measures remain updated against evolving digital complexity which often outpaces governance preparedness as cautions by the CrowdStrike outage clarified urgently.

5. BUILDING ORGANIZATIONAL RESILIENCE

5.1 Hybrid Cloud Adoption Benefits

Hybrid Cloud as the Resilience Foundation
For enterprises seeking enhanced infrastructure resilience in light of the CrowdStrike outage while retaining access to leading SaaS capabilities, hybrid cloud architectures emerge as strategic recovery vehicles offering greater redundancy and availability versus legacy hardware or single cloud vendor lock-in risks. CIOs now accelerate migration evaluating providers like Azure, AWS and Oracle for capabilities balancing security, sovereignty and flexibility for variable workloads. Benefits over legacy infrastructure include:

1. **Reduced Vendor Lock-In Risks**
   Unlike complex on-premise stacks, multi-cloud simplifies switching across platforms or scaling specific offerings to defend better against vendor-specific outages. Workload portability across Azure and AWS ensures CrowdStrike-scale failures don't paralyze entire apps if built cloud agnostic. Italicizing unique sovereignty strengths also improves resilience against regional disruption.
2. **Enhanced Cyber Resilience**
   Leading cloud providers invest over $20 billion annually in cybersecurity outpacing legacy firewall spends enabling CISOs robust, always updated threat detection versus on-premise tech stagnating fast against zero-days. Homogenized tooling like AWS Guard Duty across geo-zones outflanks malware better while enabling rapid response.

3. **Built-In Backup & Recovery**
   Legacy hardware lacked cost-efficient backup or disaster recovery capabilities for rapid restoration after incidents as applications were embedded on localized servers. Native replication, availability zones and point-in-time recovery across leading clouds allow cheap durability even when instances fail in one region due to coding errors as CrowdStrike demonstrated.
4. **Scalability Against Demand Surges**
   Spike failures saw many traditional data centers crash during peak activity moments impairing performance and forcing downtime. Multi-cloud's near infinite capacity absorbs volatile loads easily through autoscaling groups matching business needs cleaving downtime risks from usage fluctuations.
5. **Faster Deployment of Security Patches**
   Whereas cumbersome change approval processes for on-premise apps left vulnerabilities lingering for months, devops-centric cloud platforms enable continuous deployment of patches in hours once vulnerabilities surface in containers, Linux instances or node dependencies. This allows faster inoculation against threats like those faced during the CrowdStrike outage window.

By leveraging hybrid cloud's inherent flexibility, scalability and advanced continuity protections, organizations can drive resilience dramatically higher while optimizing spending previously earmarked for unwieldy DR sites, outdated hardware and fragmented security tools.

5.2 Incident Response Planning Gaps

Exposed: Shortcomings in Incident Response Programs

A sobering lesson from the CrowdStrike event showcasing digital brittleness is the wide prevalence of security gaps specifically tied to incident response, business continuity and crisis management planning methodologies currently adopted by global enterprises. With over 80% of impacted organizations reporting negative business impact exceeding $15 million in losses, deficiencies surfaced around preparedness include:

1. **Fragmented Vendor & Supply Chain Visibility**
   While disaster recovery plans have evolved to map internal assets well, lack of holistic visibility into dependencies on external vendors left many blindsided by the scale of disruption once CrowdStrike tools failed. Very few retain continuously updated external asset inventories with response impact analysis.
2. **Limited Executive Crisis Simulation Training**
   Where strong technical security teams exist, tabletop exercises evaluating leadership communications readiness during major events remain inadequate. Most CEOs lack sufficient training through crisis simulation rehearsals which manifested in poor customer messaging exacerbating outrage during the outage.
3. **Insufficient Automation in Response Playbooks**
   Manual runbooks compiled long ago crumbled under activity volumes faced during the fast-moving breach and were quickly abandoned. Lacking automation to parse threat data, orchestrate systems isolation and initiate recovery procedures saw paralysis set in instead of nimble technology-assisted response.
4. **Weaknesses Handling Third-Party Vendor Incidents**

With supply chain attacks accelerating, organizational playbooks appeared dated in handling severe vendor-originated threats like the CrowdStrike failure which required different forensics, legal and communications approaches than traditional malware response plans focus on still. Customers were often left confused by the limited visibility provided externally during the early hours.

5. **Limited Pre-Planned Failover Capabilities**
   Where failure of antivirus tools was known to potentially impair operations, few IT teams had actually conducted software failover exercises in practice to validate backup systems, procedures and workforce capability when primary defenses became unavailable unexpectedly. This manifested in delays resurrecting productivity once alerts emerged.

By revisiting contingency plans through the risk scenarios faced during this defining incident for alignment to today's interdependent ecosystems, organizations can retool preparedness matching current challenges.

5.3 Phased Deployment Strategies

Balancing Innovation & Resilience: Phased Rollouts

Among key insights from post-mortems following major business disruptions induced by technology failures is the risk of 'big bang' deployments where new software or infrastructure upgrades launch simultaneously across the entire ecosystem without insulation of potential risks. The CrowdStrike incident equally stemmed from broad rollout of a defective update without adequate fail-safes that soon crippled endpoints globally when issues emerged.

Organizations hence must strike balance between harnessing promising innovations and change while insulating overall systems from potential stability risks still maturing new tools or code may pose despite extensive testing. By adopting phased deployment strategies compartmentalizing risk below Enterprise-wide tolerances, CIOs can champion adoption while also metering exposures to drive overall resilience.

Four Pillars of Gradual Change Management

1. **Sandboxed Rollouts**
   Initially releasing changes within small, contained test groups or business units provides valuable empirical understanding of issues before enterprise-wide propagation. Observational pilot groups should mirror software diversity resembling production ecosystem to affirm portable efficacy.

2. **Progressive Feature Enablement**
   For expansive platform updates spanning hundreds of tools simultaneously like antivirus agents, opting for incremental feature activation releasing one capability a time delays risks from everything failing at once if unclear interoperability emerges between all modernization elements.

3. **Beta Subscription Groups**
   Firms often launch innovations to customers volunteering to 'opt-in' first while retaining legacy infrastructure for others till value proven. Forced big-bang mandates then appear less essential if gradual onboarding photosynhesizes adoption data at judicious cadence.

4. **Failsafe Rollback Plans**

In the event isolated issues scale into availability risks despite gating, clearly defined rollback procedures help developers rapidly reconstitute prior stable configurations temporarily if bugs endure while interrupting enterprise-wide circulation until root causes are remediated. Failsafe plans buy resilience.

While agility demands continuous integration of improvements in product lifecycles, measured change adoption balancing diversity, gating and rollback availability helps CIOs champion transformation securely when orchestrating living business ecosystems interfacing with customer needs globally across functions, without vulnerabilities snowballing as the CrowdStrike saga forewarned prudently for future generations.

6. CONCLUSION

6.1 Key Takeaways for Policymakers and Business Leaders

Key Takeaways: Fostering Collective Resilience

As policy architects stewarding critical infrastructure and business leaders harnessing technology to propel organizational success, the systemic fragilities and planning gaps exposed by the CrowdStrike case demand urgent coordinated action across public and private spheres of responsibility. Though scope remains for technical remedies addressing immediate vulnerabilities, holistic lasting resilience calls for multilateral collaboration to balance security, innovation and growth. Key imperatives include:

1. **Stress Testing Interdependence**
   Continuous stress testing mandated through regulation must address supply chain risks spanning tier-1 partners to downstream software vendors to reveal overdependence risks and drive diversification. Policy steering around redundancy requirements is equally prudent.

2. **Cyber Risk Quantification**
   Inadequate financial quantification of cyber incidents results in chronic underinvestment in resilience and response capabilities. Standardizing loss assessments and mandated disclosures will overcome opacity to help boards allocate security budgets befitting assets at risk beyond outdated PCI or HIPAA mandates insufficient to govern modern digital ecosystems.

3. **Collective Response Protocols**
   Ensuring cohesive crisis response when failures spread across multiple vendors in critical industries requires establishing clear coordination protocols and communication pipelines pre-emptively between national regulators, agencies and providers through crisis simulation exercises. Reporting standards must instill transparency balancing accountability with restoration needs sans panic.

4. **Sovereign Alternatives Development**
   Policy vision must address concentrated supply side risks in domains like antivirus, cloud and microprocessor supply chains through funded innovation of trusted domestic alternatives and open standards relaxation excessive vendor dependency risks to sustain innovation continuity without protectionism fears or compliance overheads limiting security.

5. **Resilient Tech Design Principles**
   As threats persist growing amidst heightened connectivity, resilient principles manifesting redundancy, compartmentalization and recoverability must stand embedded across infrastructure and software system design from inception itself rather than as downstream band-aid solutions. Holistic digital robustness emerges organically through better technical hygiene and modular fail-safes preventing enterprise paralysis risks seen during the CrowdStrike incident from recurring given enough forethought today.

With growing intelligence regarding systemic weaknesses exposed, we now hold opportunity to co-architect the secure digital foundations that will underpin all human progress ahead through prudent action collectively undertaken in this pivotal window of opportunity before us.

6.2 Call for Collective Action to Mitigate Future Systemic Risks

Our Shared Imperative: Architecting Resilient Futures

As interconnected risks continue growing in an era defined by digital acceleration, the fragilities laid bare by shock events like the landmark CrowdStrike outage underscore the urgent need for coordinated action reinforcing our shared ecosystem resilience. Absent multilateral collaboration across policy architects, regulators, critical infrastructure custodians and technology leaders of industry, we remain perilously vulnerable to subsequent failures propagating breakdowns across the intricate networks society now depends upon for day-to-day survival.

Yet retrospective analyses reveal that many of these capability gaps are addressable through thoughtful public-private partnerships, balanced policy interventions and system-level reengineering backed by adequate investment in vital redundancy infrastructure and response mechanisms currently lacking. By collectively marshaling resources at scale, visionary leadership can yet help inoculate global communities from ensuing threats. There equally emerges tangible opportunity to engineer resilience into the very architectural foundations and software advancements destined to drive human progress across the decades ahead if we lay the groundwork wisely from this point onward.

But incremental improvements remain inadequate when measured against the pace of risk accumulation on multiple fronts. As analogues from climate change suggest, reaching crisis inflection points may severely constrain viable response options if windows for gradual course correction go unheeded in advance. Across cybersecurity, finance, healthcare, energy and transportation domains, we require nothing less than to universally instill the cultural and technical DNA that fosters durable systems capable of handling stress, isolating failures and reconstituting functionality with agility during even extreme shock events. This demands security not be an afterthought but an integral priority spanning policy, management and technical design arenas.

With past reflecting prologue, we must evangelize the vision, investment and engineering essential to safeguard civilization’s accelerating digital foundations for generations ahead. Possibilities abound provided diverse stakeholders collectively embrace resilience as a public good meriting sustained commitment in the face of adversity. By recognizing this imperative, even enterprises primarily accountable to shareholders over public stakeholders can serve sustainability principles helping balance continuity with shareholder returns. The vital point remains to simply start our long overdue voyage without delay.

6.3 Emphasis on Learning From This Wakes-up Call to Increase Infrastructure Resilience

Learning from Near-Misses: Averting "Digital Disaster"

While dissecting the anatomical vulnerabilities behind events like the CrowdStrike failure may still dominate headlines, the deepest imperative remains learning from such near-misses to drive collective action that reinforces infrastructure stability over the horizon before cascading risks manifest at scale. Across critical domains like healthcare, transportation and financial networks, latent system fragilities persist akin to seismic fault lines needing urgent reinforcement. Though misfortune brought suffering, we yet retain agency to let insights secure civilization's accelerating digital foundations for generations ahead if we collectively center resilience as an essential public good demanding investment.

With risk trajectories remaining nonlinear, the argument for prudent augmentation of backup systems, stress testing regimes and response readiness grows only more pressing as threat vectors multiply. Much as sampling isolated malware incidents fails to convey the full extent of stealthy threat actor sophistication timed for maximal disruption, assessing the CrowdStrike outage solely on economic costs risks overlooking the long-term systemic hazards encryption failures augur if unchecked. Infrastructure custodians in particular must extrapolate scenarios highlighting potential humanitarian costs tied to digital paralysis across vital networks. This expanded lens compels urgency driving meaningful investment in systemic risk reduction well in advance of future shock events.

Equally, exercising continuity plans through simulated crisis scenarios allows organizations to uncover latent capability gaps around vital areas like executive decision protocols, third-party software dependencies, failover activation triggers and staff cross-training on secondary systems needed during prolonged primary tool outages. Very few entities conduct routine resilience fire drills today, reflecting chronic under-preparedness. Here too, disaster recovery budgets remain vestigial rather than scaled to address enterprise-wide risks, especially from vendor platform failures now needing insulation.

With past crises signaling prologue, we collectively shoulder responsibility to preempt "digital disasters" through farsighted resilience infrastructure worthy of tomorrow's hyper-connected world. The incremental costs of business continuity pale against the sweeping value at stake globally across healthcare access, transportation freedom, vibrant commerce and overall prosperity if we wait much longer to meaningfully augment cyber maturity. Core to this charge remains learning judiciously from near-misses today to erect durable systems able to withstand entropy from perils ahead, natural or human-induced. Visionary leadership now holds keys to engineer reliable foundations upholding modern life should they choose to generationally lift preparedness before periods of stability recede. The principles illuminated by watershed moments like the CrowdStrike case must indubitably light such passage.

REFERENCES

[1] 2024 CrowdStrike incident. (2024, July 25). Wikipedia. https://en.wikipedia.org/wiki/2024_CrowdStrike_incident
[2] Art. 32 GDPR – Security of processing - General Data Protection Regulation (GDPR). (2016, August 30). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-32-gdpr/
[3] Bishop, K., & Kharpal, A. (2024a, July 19). CrowdStrike issue causes major outage affecting businesses around the world. CNBC. https://www.cnbc.com/2024/07/19/crowdstrike-suffers-major-outage-affecting-businesses-around-the-world.html
[4] Bishop, K., & Kharpal, A. (2024b, July 19). CrowdStrike issue causes major outage affecting businesses around the world. CNBC. https://www.cnbc.com/2024/07/19/crowdstrike-suffers-major-outage-

affecting-businesses-around-the-world.html

[5] Chaos persists as IT outage could take time to fix, says cybersecurity firm boss. (2024, July 20). BBC News. https://www.bbc.com/news/live/cnk4jdwp49et

[6] Chen, W., & Chen, W. (2024, July 19). Microsoft outage leaves China largely untouched as tech self-sufficiency campaign pays off. South China Morning Post. https://www.scmp.com/tech/big-tech/article/3271171/microsoft-outage-leaves-china-largely-untouched-tech-self-sufficiency-campaign-pays

[7] CrowdStrike. (2024, July 20). Technical Details: Falcon Content Update for Windows Hosts. crowdstrike.com. https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/

[8] CrowdStrike backlash over "0 apology voucher for IT chaos. (2024, July 25). https://www.bbc.com/news/articles/ce58p0048r0o

[9] CrowdStrike Timeline Mystery | Bitsight. (n.d.). Bitsight. https://www.bitsight.com/blog/crowdstrike-timeline-mystery

[10] Dunstan, J., Easton, K., Janda, M., Saarinen, N., Nancarrow, D., Vyas, H., Perera, A., Johnston, G., & Ryan, B. (2024, July 19). Global IT outage: Computer havoc caused by CrowdStrike outage could take days to fix — as it happened. ABC News. https://www.abc.net.au/news/2024-07-19/global-it-outage-crowdstrike-microsoft-banks-airlines-australia/104119960

[11] Global IT Outage: Is This A Warning? - Kent Invicta Chamber of Commerce. (2024, July 23). Kent Invicta Chamber of Commerce. https://www.kentinvictachamber.co.uk/members-blog/global-it-outage-is-this-a-warning/

[12] Google Cloud Service Health. (n.d.). https://status.cloud.google.com/incidents/DK3LfKowzJPpZq4Q9YqP

[13] Hale, C. (2024, July 19). Microsoft says its cloud services are back up after major outage. TechRadar. https://www.techradar.com/pro/microsoft-says-its-cloud-services-are-back-up-after-major-outage

[14] Jennewine, J. B. B. W. a. T. (2021, December 16). Why CrowdStrike Holdings Stock Is Still Delivering Red-Hot Growth. The Motley Fool. https://www.fool.com/investing/2021/12/16/why-crowdstrike-holdings-stock-was-gaining-today/

[15] Milmo, D., Kollewe, J., Quinn, B., Ibrahim, M., & Taylor, J. (2024, July 20). Slow recovery from IT outage begins as experts warn of future risks. The Guardian. https://www.theguardian.com/australia-news/article/2024/jul/19/microsoft-windows-pcs-outage-blue-screen-of-death

[16] Newman, L. H., Burgess, M., & Greenberg, A. (2024, July 19). How One Bad CrowdStrike Update Crashed the World's Computers. WIRED. https://www.wired.com/story/crowdstrike-outage-update-windows/

[17] O'Flaherty, K. (2024, July 19). CrowdStrike Windows Outage—What Happened And What To Do Next. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2024/07/19/crowdstrike-windows-outage-what-happened-and-what-to-do-next/

[18] Online, E. (2024, July 20). Microsoft outage cause explained: What is CrowdStrike and why users are getting Windows' blue screen of de. Economic Times. https://m.economictimes.com/magazines/panache/microsoft-outage-cause-explained-what-is-crowdstrike-and-why-users-are-getting-windows-blue-screen-of-death/amp_articleshow/111858827.cms

[19] Shamsian, J. (2024a, July 19). CrowdStrike's terms and conditions say most customers would just get a refund due to the massive outage, cybersecurity lawyer says. Business Insider. https://www.businessinsider.com/crowdstrike-terms-conditions-limits-damages-to-refund-2024-7

[20] Shamsian, J. (2024b, July 19). CrowdStrike's terms and conditions say most customers would just get a refund due to the massive outage, cybersecurity lawyer says. Business Insider. https://www.businessinsider.com/crowdstrike-terms-conditions-limits-damages-to-refund-2024-7

[21] TechCrunch is part of the Yahoo family of brands. (2024, July 19). https://techcrunch.com/2024/07/19/faulty-crowdstrike-update-causes-major-global-it-outage-taking-out-banks-airlines-and-businesses-globally/

[22] Tidy, J. (2024, July 19). IT problems will take "some time" to fix, says Crowdstrike boss. BBC News. https://www.bbc.co.uk/news/articles/cn4vgq5150qo

[23] Watch Sky News live. (2024, July 19). [Video]. Sky News. https://news.sky.com/story/outages-latest-airports-business-and-broadcasters-experiencing-issues-worldwide-13180821

[24] Weston, D. (2024, July 20). Helping our customers through the CrowdStrike outage - The Official Microsoft Blog. The Official Microsoft Blog. https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

[25] Williams, K. (2024, July 24). CrowdStrike losses may be biggest test yet of cybersecurity insurance

risk warning from Warren Buffett. CNBC. https://www.cnbc.com/2024/07/24/crowdstrike-biggest-test-yet-for-cyber-insurance-buffett-warned-about.html

[26] Wright, R. (2024, July 19). “Bedlam”: Grounded flights and check-in chaos at airports all over Europe due to major IT outage. Euronews. https://www.euronews.com/travel/2024/07/19/microsoft-outage-flight-delays-and-cancellations-arrive-at-the-airport-early-say-airlines

[27] x.com. (n.d.-a). X (Formerly Twitter). https://x.com/George_Kurtz/status/1814235001745027317

[28] x.com. (n.d.-b). X (Formerly Twitter). https://x.com/Ryanair/status/1814284604385186237

[29] Yeo, A. (2024, July 19). Windows PCs crashing worldwide due to CrowdStrike issue. Mashable ME. https://me.mashable.com/tech/44300/windows-pcs-crashing-worldwide-due-to-crowdstrike-issue