PROBLEMS

INTRODUCTION

Crowdstrike. An American software company hardly visible to the naked eye, but the life blood essential to the seamless global flow of safe digital transactions that are properly executed every millisecond. But on July 19th, this unbeknownst company would make its grand appearance to the world. Only its reveal would take place on a day where their services take lives, billions, and many unanswered questions down in an event known to be the worst fail in software history. For days, thousands stranded in airports, 911 calls left unanswered, billions of dollars lost, cancellations in hospitals, and millions of computers left unfixable.

In recent standards, Crowdstike has met the golden standard for an ultra growth tech stock. Returning an absolutely stunning 310.62% return in 6 short years[1]. But how could this golden egg of American tech plummet so quickly? How could we prevent this in the future? How much damage did crowdstrike really cause on July 19th?

Crowdstrike isn't just one large IT accident. It's a lesson revealing large cracks in our world that we are still not immune to the brutal consequences of even the tiniest mistake.

COMPANY BACKGROUND

Crowdstrike

CrowdStrike is a leading cybersecurity company that focuses on protecting computers and other devices connected to the internet from cyberattacks. Specializing in cloud-based endpoint protection, it utilizes advanced technologies to prevent ransomware, viruses, and unauthorized access before damage is caused. [2]As of November 17, CrowdStrike had a market cap of $82.5 billion, making it one of the largest and most influential companies in the cybersecurity and cloud computing industries. Its services are crucial for industries such as healthcare, finance, and government, areas in which protecting user data is of utmost importance.

Microsoft

Microsoft is a global tech leader, started in 1975 by Bill Gates and Paul Allen. Known mostly for creating the Windows graphical operating system. Microsoft has expanded into cutting edge fields, including Artificial Intelligence (AI), cloud services with Azure, and hardware such as Surface devices and the

---

[1] "CrowdStrike Holdings, Inc. (CRWD) Stock Price, News, Quote & History - Yahoo Finance." *Finance.yahoo.com*, finance.yahoo.com/quote/CRWD/.

[2] CrowdStrike. CrowdStrike: Cybersecurity for the Modern Era. CrowdStrike, https://www.crowdstrike.com/en-us/. Accessed 5 Jan. 2025.

beloved XBox[3]. As of November 17, it has a market cap of $3.085 trillion dollars, as well as an impressive resume being utilized by major companies such as Starbucks, BMW, and NASA.

DISCUSSION OF THE PROBLEM

Overview of the Problem

The crowdstrike outage began on July 19th, 2024, 04:09 UTC. After a faulty, unchecked software is released to the world, a logic error begins to jam many Microsoft PC's. Instantly, 8.5 million devices are found on a notorious "death screen", leading to many airports, hospitals, and banks unable to function[4].

"How could an incredibly unknown company release a minor update that breaks 8.5 million computers in a matter of seconds?" Due to an unforgiving cascade of effects, such as a high delay in solution, terrible timing, untested software practices, heavy reliance on invasive cybersecurity software, and many more cumulative reasons, we find ourselves with the perfect storm to temporarily shut down a multi-trillion dollar industry.

Delay of a Solution & Increase in Cyberattacks

Although the attack happened on July 19, companies took up to weeks to recover from the outage. US tech expert Simon Pardo predicted that recovery could take "more than a few weeks to resolve this issue entirely"[5] depending on the size of the affected business/organization. Smaller and medium-sized businesses without dedicated IT teams struggled to get back on track, while larger companies like American Airlines addressed the outage more swiftly.

But why did it take so long to find a solution? Initially thought of as an easy fix- a simple deletion of the malfunctioning file in the update- it soon became clear that it would be much more difficult to tackle: the Windows operating system crashed each time it was rebooted, preventing the fix from being done remotely[6]. Cybersecurity researcher Kevin Beaumont explained that each system impacted by the outage would have to enter 'Safe Mode' and then reboot to remove the update, a process extremely lengthy and inefficient[7].

The delay of a solution also increased the exposure of cyberattacks against Crowdstrike customers. The UK Cyber Security Center has reported an increase of phishing attempts and external attacks attempting

---

[3] Microsoft. Business Description: Annual Report 2012. Microsoft, https://www.microsoft.com/investor/reports/ar12/financial-review/business-description/index.html. Accessed 5 Jan. 2025.

[4] Umbelino, Pedro. "CrowdStrike Outage Timeline and Analysis | Bitsight." *Bitsight*, 24 July 2024, www.bitsight.com/blog/crowdstrike-outage-timeline-and-analysis.

[5] The Feed. "Microsoft's CrowdStrike Issue Can Take Weeks to Fix, Claim Experts; Here's What You Can Do in the Meantime." *The Economic Times*, Economic Times, 20 July 2024, economictimes.indiatimes.com/news/international/us/microsofts-crowdstrike-issue-can-take-weeks-to-fix-claim-experts-heres-what-you-can-do-in-the-meantime/articleshow/111888991.cms?from=mdr. Accessed 16 Dec. 2024.

[6] Kubota, Taylor. "A Computer Scientist's Take on the CrowdStrike Crash." *Stanford Report*, Stanford University, 26 July 2024, news.stanford.edu/stories/2024/07/an-expert-s-overview-of-the-crowdstrike-outage.

[7] Tidy, Joe. "IT Problems Will Take "Some Time" to Fix, Says Crowdstrike Boss." *BBC*, BBC, 19 July 2024, www.bbc.com/news/articles/cn4vgq5150qo.

to take advantage of companies, businesses, and individuals[8]. Gartner analyst Eric Grenier has warned against accepting help from non-Crowdstrike related individuals, stressing the importance of only engaging with those from Crowdstrike[9]. Crowdstrike CEO George Kurtz cautioned that "adversaries and bad actors will try to exploit events like this" and has encouraged customers to "remain vigilant and ensure that you're engaging with official CrowdStrike representatives"[10]

Industries/People Affected by the Outage

1. Health Care/Medical services - Michelle

The healthcare industry was among the hardest industries impacted by the outage. Hospitals across the world were forced to cancel surgeries and appointments, while some were unable to receive 911 emergency calls. Healthcare facilities and hospitals in the US, UK, Germany, Austria, and Israel were just some of the impacted locations[11]. Many medical records were unable to be accessed during this time, leading to the cancellation of non-urgent procedures, appointments, and surgeries. However, patients with urgent procedures faced danger, as hospitals struggled with "where to send critically ill patients as several operating rooms had been shut down" [12]. One such case was 73 year old Gary Baulos, who was scheduled for an open heart surgery. However, due to the outage, the surgery was canceled and unable to be rescheduled. His daughter, Alison Baulos, voiced her concern that issues like the outage could determine between life or death[13].

Furthermore, 911 services, particularly in Alaska, New Hampshire, Texas, and Ohio, had also been reported inactive and malfunctioning[14]; after systems began to go back to normal, emergency services and

---

[8] Koenig, David , and Jill Lawless. "Malicious Actors Trying to Exploit Global Tech Outage for Their Own Gain." *AP News*, The Associated Press, 20 July 2024, apnews.com/article/crowdstrike-microsoft-outage-software-update-ebcba985600530a4689289eae38619bf.

[9] Koenig, David , and Jill Lawless. "Malicious Actors Trying to Exploit Global Tech Outage for Their Own Gain." *AP News*, The Associated Press, 20 July 2024, apnews.com/article/crowdstrike-microsoft-outage-software-update-ebcba985600530a4689289eae38619bf.

[10] CrowdStrike. "Falcon Content Update Remediation and Guidance Hub | CrowdStrike." *Crowdstrike.com*, 6 Aug. 2024, www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/.

[11] Halpern, Luke. "CrowdStrike Reports Global Outage, Affecting Hospitals, Businesses across the World." *Pharmacy Times*, MJH Life Sciences, 19 July 2024, www.pharmacytimes.com/view/crowdstrike-reports-global-outage-affecting-hospitals-businesses-across-the-world. Accessed 16 Dec. 2024.

[12] "Surgeries and Doctor's Appointments Canceled amid Global IT Outage." NBC News, 19 July 2024, www.nbcnews.com/health/health-news/global-it-outage-us-hospitals-surgery-appointments-cancellations-rcna162687.

[13] NBC News. "Major Global IT Outage Grounds Flights, Hits Banks and Businesses around the World." *NBC News*, 20 July 2024, www.nbcnews.com/news/world/live-blog/live-updates-it-outage-flights-banks-businesses-microsoft-crowdstrike-rcna162669.

[14] Halpern, Luke. "CrowdStrike Reports Global Outage, Affecting Hospitals, Businesses across the World." *Pharmacy Times*, MJH Life Sciences, 19 July 2024, www.pharmacytimes.com/view/crowdstrike-reports-global-outage-affecting-hospitals-businesses-across-the-world. Accessed 16 Dec. 2024.

experts requested that “people should not try calling 911 to test the system”[15]. Fortunately, many 911 emergency services were down in less than 24 hours.

2. Airlines - Kendall

The Crowdstrike incident caused massive disruptions for airlines and public transport systems worldwide. An update to Crowdstrike’s software disrupted Microsoft's Windows operating system, which many airlines depend on for important functions like reservations and flight scheduling. While the Federal Aviation Administration (FAA), airports, and airlines experienced no major technical issues regarding flight controls, coordination between all systems is essential for smooth and on-time flights. Since airline staff could not access flight or passenger information, thousands of flights were canceled or delayed[16].

3. Companies - Kendall

The global IT outage associated with Crowdstrike is expected to cost the Fortune 500 companies, excluding Microsoft, a minimum of $5.4 billion in direct financial losses. According to Jonathan Hatzor, co-founder and chief executive officer at Parametrix, “CrowdStrike cannot take the liability for all of the financial impact and all of their clients in an unlimited way … And it’s impossible for companies to carry so much risk”. All of these outages include cyber insurance policy payouts. However, cyber insurance will only cover 10% to 20% of the losses and between $400 million and $1.5 billion losses; this event may have been the worst losses in the industry in over 20 years. The rest of the losses will happen at the liability of many Fortune 500 companies. The healthcare sector accounts for $1.94 billion in losses at a clip of $64.6 million per healthcare company. Banking struggled as well, but airlines have the highest per company costs[17].

CONCLUSION

July 19th will serve as a cautionary tale to the world of tech for many years to come. Whether it’s the numerous vulnerabilities and possibilities still waiting to be patched, or the pioneers who innovate solutions to protect us in the future, it is clear that this isn’t just a tale; but a call to action. Software companies will be encouraged to check loose links, and employee’s will be forced into more rigorous sandbox testing before deployment. With new innovation creates tighter room for reliance and sole ability for minor issues to affect large bodies of people.

Moreover, our world won’t just be ready to prevent, but also to receive massive IT issues like July 19th. Rather than taking weeks to resolve these problems, there will be safety mechanisms and nets to prevent them in seconds.

---

[15] NBC News. “Major Global IT Outage Grounds Flights, Hits Banks and Businesses around the World.” *NBC News*, 20 July 2024, www.nbcnews.com/news/world/live-blog/live-updates-it-outage-flights-banks-businesses-microsoft-crowdstrike-rcna162669.

[16] Wichter, Zach. “Airlines Rely on Complex Systems: Why the CrowdStrike Hiccup Could Cause Days of Chaos.” *USA TODAY*, USA TODAY, 19 July 2024, www.usatoday.com/story/travel/airline-news/2024/07/19/airline-tech-glitch-flight-chaos/74471167007/.

[17] Jones, David. “CrowdStrike Disruption Direct Losses to Reach $5.4B for Fortune 500, Study Finds.” *Cybersecurity Dive*, 25 July 2024, www.cybersecuritydive.com/news/crowdstrike-cost-fortune-500-losses-cyber-insurance/722396/.

But July 19th is also a reminder of wildcards, demonstrating to us that we are never safe from some of the most pressing and quickly destructive issues our world will face. We can never be prepared for

DISCUSSION QUESTIONS

1. What should companies in the same field as Crowdstrike do in the future to prevent issues like this?
2. How can companies improve their response strategies to minimize the damage and recovery time in the event of a similar outage.

SOLUTIONS

INTRODUCTION

What happens when the digital systems we depend on everyday suddenly fail? On July 19, 2024, the world found out. Crowdstrike, a top cybersecurity company that protects internet devices from cyberattacks, was itself compromised by a catastrophic software error. After an untested and defective software was launched, a programming flaw caused millions of Microsoft PCs to malfunction, triggering chaos on a global scale[18]. Many industries that rely on Microsoft systems were unable to function. Crowdstrike's delay in implementing a solution further increased the vulnerability of its customers, exposing them to additional cyberattacks. After the outage, recovery took weeks, with smaller companies without IT struggling even more to regain normal operations[19].

To prevent such failures, Crowdstrike could have implemented sandboxing and telemetry-based monitoring, which could have caught the error before it affected millions.

OVERVIEW OF PROBLEM

The crowdstrike outage began on July 19th, 2024, 04:09 UTC. Crowdstrike's Falcon Sensor (which continuously checks for malicious software) is deployed on millions of computers that run Microsoft Windows (and other popular operating systems that weren't affected). After a faulty, unchecked software update was deployed to the sensor, logic errors began to jam many Microsoft PC's. Instantly, 8.5 million devices are found on a notorious "death screen", leading to many airports, hospitals, and banks unable to function[20].

"How could an incredibly unknown company release a minor update that breaks 8.5 million computers in a matter of seconds?" Due to an unforgiving cascade of effects, such as a high delay in solution, terrible timing, untested software practices, heavy reliance on invasive cybersecurity software, and many more cumulative reasons, we find ourselves with the perfect storm to temporarily shut down a multi-trillion dollar industry[21].

After releasing a faulty global software update in their Crowdstrike Falcon Sensor, a minor error (that resulted in an out-of-bounds memory error) was responsible for most of the damage. Although the software error could have been easily fixed and revised, deploying an error-riddled software will jam many machines that run on this software. Since the Crowdstrike Falcon Sensor was deployed on a global level to monitor and safeguard machines like Microsoft PC's, an unlodgeable error screen was visible to millions including ones in airports and hospitals[22]

---

[18] Krebs, Brian. "Global Microsoft Meltdown Tied to Bad CrowdStrike Update." Krebs on Security, 7 July 2024, krebsonsecurity.com/2024/07/global-microsoft-meltdown-tied-to-bad-crowstrike-update/.
[19] Smith, Jennifer. "CrowdStrike Aftermath: Lessons from the IT Outage." HBS Blog, hbs.net/blog/crowdstrike-aftermath-it-outage.
[20] Umbelino, Pedro. "CrowdStrike Outage Timeline and Analysis | Bitsight." Bitsight, 24 July 2024, www.bitsight.com/blog/crowdstrike-outage-timeline-and-analysis.
[21] Kerner, Sean Michael. "CrowdStrike Outage Explained: What Caused It and What's Next." TechTarget, 26 July 2024, www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.
[22] Jones, David. "CrowdStrike Blames Mismatch in Falcon Sensor Update for Global IT Outage." Cybersecurity Dive, 7 Aug. 2024, www.cybersecuritydive.com/news/crowdstrike-mismatch-falcon-sensor-outage/723569/.

Had the software just been meticulously tested, run through a sandbox deployment environment, or quickly recovered within minutes of deployment, the crowdstrike disaster could have been something invisible to the eye of the public.

MARKET TRENDS

Although the Crowdstrike outage was one of the largest disruptions, there have been similar, smaller outages in the past involving companies such as Facebook (META), Google, British Airways, Fastly, Dyn, and more. However, due to limited technology, the large impact of these attacks were unable to be measured accurately and were underestimated.

In October of 2021, billions of Facebook (META) users and Facebook-login platforms were unable to access their Facebook accounts due to a "configuration change to the backbone routers" that guided network traffic[23]. This change created a domino effect, impacting all of Facebook's services, including Instagram, WhatsApp, and Messenger. Despite the outage being only six to seven hours, Facebook "lost $47.3 billion in market value", losing Mark Zukerberg "an estimated $6 billion"[24]. Although it is unknown exactly how large businesses and industries were hit, the outage impacted billions of users worldwide.

The outage/attack with the most similar consequences was the Dyn DDoS attack. On October 21, 2016, the servers of internet company Dyn shut down, causing popular sites like Netflix, Reddit, Twitter, and CNN to be inaccessible in the US and Europe[25]. Mirai, the malicious software behind the distributed denial of service (DDoS) attack, infected a network of Dyn's computers with high levels of traffic, eventually leading Dyn to face "substantial business interruption issues, recovery costs and reputational damages from the attack"[26]. An average of $2.5 million for organizations/businesses was the estimated cost of recovery for the incident, while Dyn's cost was guessed to be more than $2.5 million[27]. Furthermore, about 8%, or 14,000, of internet platforms ceased to use Dyn following the attack. As reliance on technology increased each year, concerns regarding maintenance systems and commands surged, resulting in a growth of significance for cybersecurity and internet safety.

---

[23] Taylor, Josh. "Facebook Outage: What Went Wrong and Why Did It Take so Long to Fix after Social Platform Went Down?" *The Guardian*, 5 Oct. 2021, www.theguardian.com/technology/2021/oct/05/facebook-outage-what-went-wrong-and-why-did-it-take-so-long-to-fix.

[24] Carpenter, Scott. "Zuckerberg Loses $6 Billion in Hours as Facebook Plunges." *Bloomberg.com*, 4 Oct. 2021, www.bloomberg.com/news/articles/2021-10-04/zuckerberg-loses-7-billion-in-hours-as-facebook-plunges.

[25] Woolf, Nicky. "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say." *The Guardian*, The Guardian, 26 Oct. 2016, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[26] Young, Kelli. "Cyber Case Study: The Mirai DDoS Attack on Dyn." *CoverLink Insurance*, CoverLink Insurance, 10 Jan. 2022, coverlink.com/case-study/mirai-ddos-attack-on-dyn/.

[27] Young, Kelli. "Cyber Case Study: The Mirai DDoS Attack on Dyn." *CoverLink Insurance*, CoverLink Insurance, 10 Jan. 2022, coverlink.com/case-study/mirai-ddos-attack-on-dyn/.

SOLUTIONS

MAIN SOLUTION - SANDBOX

Crowdstrike could have mitigated the catastrophic July 2024 outage by incorporating sandboxing, alongside other incident response and preparedness measures. Sandboxing is a practice where updates are tested in isolated environments that closely mirror real-world conditions. This would have allowed for the company to identify the out-of-bounds memory error within the Falcon Sensor[28] update preceding the global update in turn preventing the shutdown of 8.5 million computers[29].

Additionally, integration of sandbox testing with telemetry-based monitoring(ability to remotely monitor the security, health and performance of applications[30] would have enabled real-time detection of faults in the testing phase, allowing Crowdstrike developers to address critical issues before deployment, thus presenting errors like that of before occurring. We can also see this, having been previously done to a lower scale with small sandboxes being set up in May, if more was done in this direction, it could have potentially averted the crisis.[31]

Beyond preventing specific incidents like the July 2024 outage, the implementation of sandboxing and telemetry-based monitoring could have set a strong precedent for proactive cybersecurity practices across the industry. Through establishing a rigorous testing framework(similar to stress tests in finance[32]), Crowdstrike could ensure a higher standard of reliability and security for its products, bolstering customer trust and minimizing reputational damage as seen with their rapid stock price fall[33]. Learning from this incident, companies could view such investments as not only a means of avoiding future outages but also as an opportunity to enhance operational resilience and lead the industry in innovation.[34]

---

[28] Jones, David. “CrowdStrike Blames Mismatch in Falcon Sensor Update for Global IT Outage.” Cybersecurity Dive, 7 Aug. 2024, www.cybersecuritydive.com/news/crowdstrike-mismatch-falcon-sensor-outage/723569/.
[29] Tan, Aaron. “CrowdStrike Update Snafu Affected 8.5 Million Windows Devices.” ComputerWeekly.com, 2024, www.computerweekly.com/news/366596373/CrowdStrike-update-snafu-affected-85-million-Windows-devices.
[30] Barney, Nick. “What Is Telemetry and How Does It Work?” WhatIs.com, Dec. 2022, www.techtarget.com/whatis/definition/telemetry.
[31] Pan, Ted. “Detecting and Remediating Threats with CrowdStrike Endpoint Detection and Response.” Crowdstrike.com, 2 May 2024,
[32] *"Stress Testing." Investopedia*, n.d., https://www.investopedia.com/terms/s/stresstesting.asp. Accessed 5 Jan. 2025.
[33] *"Here's What the July Outage Affecting CrowdStrike Taught the Cybersecurity Industry." Yahoo Finance*, 2024, https://finance.yahoo.com/news/heres-july-outage-affecting-crowdstrike-082000778.html. Accessed 5 Jan. 2025.
[34] "CrowdStrike Mismatch Causes Falcon Sensor Outage." Cybersecurity Dive, 2024, https://www.cybersecuritydive.com/news/crowdstrike-mismatch-falcon-sensor-outage/723569/. Accessed 5 Jan. 2025.

GOVERNMENT INTERVENTION

Due to the reliance of government agencies and vital entities relying on compaies like Crowdstrike, it is necessary that government regulation is implemented to handle situations such as technological outages. 82% of US state governments rely on Crowdstrike alone, while 48% of half of the largest US cities utilize Crowdstrike[35]. Multiple other countries across the globe such as the United Kingdom and India also rely on Crowdstrike for their services, marking its importance on an international scale[36]. In comparison, currently, only 40%, or 20 of US states have cybersecurity laws in place.

American citizens have also voiced their concern over US cybersecurity; according to a poll done in August 2024, 62% reported a growth in concern over "both the security of federal government IT systems and the stability of critical infrastructure" after the outage. 65% support an altered approach to Microsoft product usage in government, while 46% voiced that additional protection measures were needed[37].

Countries such as the EU already have policies such as the Cyber Resilience Act (CRA), which focuses on the hardware and software products related to cybersecurity[38], and the Network and Information System 2 Directive (NIS2), a measure aimed at "boosting cybersecurity levels in the EU"[39]. Proper implementation "combined with better preparedness and a concerted effort to expand the number of trusted security software providers" is hoped to address technological outages[40]. In the US, laws and commissions such as the Executive Order on Improving the Nation's Cybersecurity, the Security and Exchange Commission (SEC), and the Security and Privacy Controls for Information Systems and Organizations have kept cybersecurity levels in check over the years. For example, the Security and Exchange Commission (SEC) ensures that businesses and companies report any cyberattacks within a certain amount of days[41] while the Security and Privacy Controls for Information Systems and Organizations set guidelines providing organizations with "a comprehensive set of best practices for

---

[35] "State and Local Government | CrowdStrike." *Crowdstrike*, 2024, www.crowdstrike.com/en-us/solutions/state-local-government/. Accessed 15 Dec. 2024.

[36] 6sense. "Crowdstrike - Market Share, Competitor Insights in Endpoint Protection." *6sense.com*, 6sense, 2024, 6sense.com/tech/endpoint-protection/crowdstrike-market-share.

[37] Chavez, Krista. "New Poll: Americans Concerned about Government Cybersecurity Following Microsoft-Crowdstrike Outage - NetChoice." *NetChoice*, NetChoice, 9 Sept. 2024, netchoice.org/new-poll-americans-concerned-about-government-cybersecurity-following-microsoft-crowdstrike-outage/.

[38] European Commission. "Cyber Resilience Act | Shaping Europe's Digital Future." *European Commission*, 15 Sept. 2022, digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[39] ---. "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) | Shaping Europe's Digital Future." *European Commission*, 21 Nov. 2024, digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[40] Pupillo, Lorenzo. "Following July's CrowdStrike Outage, This Is How We Can Avoid the next "Blue Friday."" *CEPS*, CEPS, 14 Oct. 2024, www.ceps.eu/following-julys-crowdstrike-outage-this-is-how-we-can-avoid-the-next-blue-friday/.

[41] Kovacs, Eduard. "SEC Shares Important Clarifications as New Cyber Incident Disclosure Rules Come into Effect." *SecurityWeek*, SecurityWeek, 18 Dec. 2023, www.securityweek.com/sec-shares-important-clarifications-as-new-cyber-incident-disclosure-rules-come-into-effect/.

protecting systems from cyberattacks"[42]. Although government intervention will not eliminate all cybersecurity attacks or outages, they will assist in decreasing the levels of technological difficulties.

PUNCHLINE INFO

Crowdstrike was one of thousands of companies that work behind the scenes on the illusively seamless world visible to the naked eye. But the danger of its anonymity accentuates the fact that we are far from protected from the issues that happen in aspects of our infrastructure that we don't even know exist. The Crowdstrike Falcon Sensor is one of the many services that is offered in the Cybersecurity industry, making us wonder, "How many unpatched holes are there that may cause disaster in the future?"

For example, in 2010 while many were asleep the stock market crashed by one trillion dollars in value and recovered before everybody woke up. This example alone demonstrates the high volatility that occurs in markets and technology that little know exist.

We should be looking to patch as many holes as we can in these invisible industries, including trade networks, cybersecurity software, and high frequency trading. In addition, we should be able to catch these mistakes extremely quickly, minimizing the impact and effect on the millions who use these vital softwares. This way our economy can run more seamlessly without worrying about the devastating Black Swan Events like the Crowdstrike outage.

CONCLUSION

As technology becomes a more prevalent part of daily life, it is essential that the proper standards and methods are set to ensure that technological attacks and outages are minimized. Through the Crowdstrike outage, the detrimental impacts of technology were all the more highlighted, emphasizing the importance of proper maintenance, performance monitoring, and government regulation. Practices like sandboxing can assist tech companies with preventing these outages, while approaches such as government policies can ensure that companies are following ethical and practical cybersecurity guidelines to minimize any accidents. All in all, the Crowdstrike outage has taught all the importance of online security, further helping companies become better equipped to face future challenges and adapt to a digital world.

[42] Brands, Michael . "Cybersecurity Laws and Legislation (2023) | ConnectWise." *ConnectWise*, ConnectWise, 6 May 2024, www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation.