MEMO

To Investment Team

From Your Name

Date July 19, 2024

Subject Impact of CrowdStrike Outage on Airlines and Financial Services

---

### Overview

On July 19, 2024, a global IT outage caused by a software update from cybersecurity firm CrowdStrike (CRWD) severely impacted multiple industries, including airlines, financial services, healthcare, and government agencies. The outage was triggered by a defect in a content update for Windows hosts, affecting Microsofts customers. Despite a fix being deployed, the incident has highlighted the vulnerabilities inherent in our increasingly digital and interconnected world.

### Key Events

#### Airlines

1. Major U.S. airlines such as American Airlines (AAL), Delta (DAL), and United (UAL) grounded flights.
2. Airports worldwide, including Los Angeles, Singapore, Hong Kong, Amsterdam, and Berlin, reported delays and disruptions.
3. Manual check-ins were required at several airports, causing significant delays.

#### Financial Services

1. Banks and financial services companies across Australia, India, and Germany experienced disruptions.
2. The London Stock Exchange Group (LSEG) faced data and service outages, affecting financial markets.

#### Healthcare and Government

1. Booking systems for doctors in Britain were offline.
2. Sky News and other broadcasters were taken off air.
3. Government agencies, including the Dutch and UAE foreign ministries, reported disruptions.

### Current Status

* Services are gradually being restored. Companies like American Airlines, Frontier, Spirit, Dubai International Airport, and Commonwealth Bank have reported a return to normal operations.
* CrowdStrikes CEO, George Kurtz, has apologized and confirmed that the issue was due to a software bug, not a cyberattack. However, he warned that some companies might face ongoing issues.

### Market Impact

* CrowdStrikes shares dropped by 14.5, wiping out approximately 12.2 billion in market value.
* Competitors like SentinelOne and Palo Alto Networks saw their shares rise by 10 and 2.6, respectively.
* Microsoft shares were down by 1.5.

### Potential Conclusions

1. Increased Scrutiny on Cybersecurity Firms

* This incident will likely lead to increased scrutiny and regulatory oversight of cybersecurity firms.
* Companies might diversify their cybersecurity solutions to mitigate risks associated with reliance on a single provider.

1. Investment Opportunities

* Competitors of CrowdStrike, such as SentinelOne and Palo Alto Networks, may see increased demand for their services.
* There may be opportunities to invest in companies that provide diversified cybersecurity solutions.

1. Sector Vulnerabilities

* The incident underscores the vulnerabilities in sectors heavily reliant on digital infrastructure.
* Companies in critical sectors like airlines, financial services, and healthcare may need to invest more in robust IT and cybersecurity measures.

### Action Items

1. Review Current Holdings

* Assess the impact of the outage on our current investments in affected sectors, particularly in airlines and financial services.
* Evaluate the performance and risk exposure of our investments in cybersecurity firms, including CrowdStrike.

1. Explore New Investments

* Consider increasing our positions in cybersecurity firms that have shown resilience or benefited from the incident, such as SentinelOne and Palo Alto Networks.
* Look into companies that offer diversified cybersecurity solutions to mitigate single-provider risks.

1. Engage with Portfolio Companies

* Encourage portfolio companies to review and strengthen their IT and cybersecurity protocols.
* Advise on the potential need for diversifying cybersecurity solutions to prevent similar disruptions in the future.

---

### Conclusion

The CrowdStrike outage has exposed significant vulnerabilities in our digital infrastructure, particularly in critical sectors like airlines and financial services. While the immediate impact is being mitigated, the long-term implications for cybersecurity practices and investment strategies are profound. We must proactively address these risks and explore new opportunities to strengthen our portfolio against future disruptions.

---

Your Name

Your Position

Your Contact Information