Memo to the Investment Team

To Investment Team

From Your Name

Date Current Date

Subject Analysis of CrowdStrike Outage and Its Implications

### Overview

On July 19, 2024, a significant global IT outage, triggered by a software update from CrowdStrike, disrupted various industries including airlines, financial services, healthcare, and government agencies. The event caused widespread system failures, grounding flights, halting financial transactions, and affecting healthcare services.

### Key Events

#### 1. Cause of Outage

* The outage was caused by a defective content update for Windows hosts from CrowdStrikes Falcon software.
* The issue was not a cyberattack but a software bug that led to system crashes and the infamous blue screen of death.

#### 2. Industries Impacted

* Airlines

Major U.S. airlines like American Airlines, Delta, and United grounded flights. Airports worldwide, including those in Los Angeles, Singapore, Hong Kong, Amsterdam, and Berlin, reported delays.

* Financial Services

Banks and financial services from Australia to Germany experienced disruptions, affecting transactions and customer access.

* Healthcare

Booking systems for doctors in Britain were offline, and hospitals faced challenges in accessing patient records and booking appointments.

* Government Agencies

Various government departments, including the Dutch and UAE foreign ministries, reported disruptions.

#### 3. Company Response

* CrowdStrike CEO George Kurtz publicly apologized and clarified that the issue was identified and a fix was deployed.
* The company is working individually with affected customers to restore systems, though some may face prolonged recovery times.

#### 4. Market Reaction

* CrowdStrikes shares dropped by 14.5, wiping 12.2 billion off its market value.
* Competitors like SentinelOne and Palo Alto Networks saw their shares rise, indicating a potential shift in market confidence.

### Potential Conclusions

#### 1. Operational Risks

The incident highlights the operational risks associated with software updates in critical cybersecurity tools. It underscores the need for rigorous testing and phased rollouts to mitigate such risks.

#### 2. Market Perception

The significant drop in CrowdStrikes stock indicates a loss of investor confidence. This could be an opportunity for competitors to gain market share.

#### 3. Regulatory and Legal Implications

Given the widespread impact, CrowdStrike may face legal actions from affected industries, particularly airlines and financial services. This could lead to substantial financial liabilities and regulatory scrutiny.

#### 4. Sector-Wide Review

The incident may prompt a sector-wide review of cybersecurity protocols and the reliance on single vendors for critical security updates. Diversification of cybersecurity tools might become a priority for many organizations.

### Action Items

1. Monitor CrowdStrikes Recovery Efforts

Track the companys progress in resolving the issue and restoring customer systems. Assess any further impact on their market position and customer trust.

1. Evaluate Competitor Opportunities

Analyze the performance and market positioning of competitors like SentinelOne and Palo Alto Networks. Consider potential investment opportunities in these firms as they may benefit from the fallout.

1. Assess Legal and Regulatory Developments

Stay informed about any legal actions or regulatory changes that may arise from this incident. Evaluate the potential financial impact on CrowdStrike and the broader cybersecurity sector.

1. Review Portfolio Exposure

Reassess our portfolios exposure to companies heavily reliant on single cybersecurity vendors. Consider diversifying investments to mitigate similar risks in the future.

1. Engage with Industry Experts

Consult with cybersecurity experts to understand the long-term implications of this outage and identify best practices for managing similar risks in our investments.

### Conclusion

The CrowdStrike outage serves as a critical reminder of the vulnerabilities in our interconnected digital infrastructure. While it presents challenges, it also offers opportunities to reassess and strengthen our investment strategies in the cybersecurity sector. Immediate actions and continuous monitoring will be essential to navigate the potential impacts and capitalize on emerging opportunities.

Your Name

Your Position

Your Contact Information

Please let me know if you need further details or specific analyses on any aspect of this incident.