Memo

To Investment Team

From Your Name

Date July 19, 2024

Subject Impact of CrowdStrike Outage on Key Sectors and Potential Action Items

---

### Overview

On July 19, 2024, a global IT outage caused by a software update from cybersecurity firm CrowdStrike (CRWD) led to significant disruptions across multiple industries, including airlines, financial services, healthcare, and government agencies. The outage lasted several hours before services began to be restored. The incident highlights the vulnerabilities associated with the increasing reliance on interconnected digital technologies.

### Key Events

#### 1. Cause of Outage

* A defective content update for Windows hosts from CrowdStrike triggered widespread system failures.
* CrowdStrike CEO George Kurtz confirmed the issue was a software bug, not a cyberattack.

#### 2. Impact on Industries

* Airlines

Major U.S. carriers such as American Airlines (AAL), Delta (DAL), and United (UAL) grounded flights. Airports worldwide, including Los Angeles, Singapore, Hong Kong, Amsterdam, and Berlin, experienced delays due to manual check-ins.

* Financial Services

Banks and financial institutions in Australia, India, and Germany reported disruptions. The London Stock Exchange Group (LSEG) faced data service outages.

* Healthcare

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

* Government Agencies

The Dutch and UAE foreign ministries reported disruptions.

#### 3. Restoration of Services

* By the end of the day, several companies, including American Airlines, Frontier, Spirit, Dubai International Airport, and Commonwealth Bank of Australia, reported a return to normal operations.
* CrowdStrikes competitors, SentinelOne and Palo Alto Networks, saw their shares rise, while CrowdStrikes shares dropped by 14.5.

### Potential Conclusions

#### 1. Sector Vulnerability

The incident underscores the critical vulnerabilities in sectors heavily reliant on digital infrastructure. The ripple effect of such outages can lead to significant operational and financial disruptions.

#### 2. Market Reactions

CrowdStrikes market value dropped significantly, losing 12.2 billion. This could lead to a reevaluation of dependency on single cybersecurity providers and may benefit competitors.

#### 3. Regulatory Scrutiny

Increased regulatory scrutiny on cybersecurity protocols and the robustness of IT infrastructure across industries is likely. This could lead to new compliance requirements and standards.

### Action Items

#### 1. Portfolio Review

Assess the exposure of our portfolio to companies heavily reliant on digital infrastructure. Identify potential vulnerabilities and consider diversifying investments to mitigate risks.

#### 2. Investment Opportunities

Explore investment opportunities in cybersecurity firms that could benefit from increased demand for robust security solutions. SentinelOne and Palo Alto Networks are immediate candidates given their positive market response.

#### 3. Engage with Affected Companies

Initiate discussions with companies in our portfolio affected by the outage to understand their contingency plans and measures to prevent future disruptions. This will help in assessing their resilience and long-term viability.

#### 4. Monitor Regulatory Developments

Stay informed about potential regulatory changes in cybersecurity and IT infrastructure standards. This will help in anticipating market shifts and adjusting our investment strategy accordingly.

#### 5. Risk Management

Encourage companies in our portfolio to conduct thorough risk assessments and implement robust cybersecurity protocols. This proactive approach can mitigate the impact of similar incidents in the future.

### Conclusion

The CrowdStrike outage serves as a stark reminder of the interconnected risks in our digital economy. While the immediate impact is significant, it also presents opportunities for strategic investments and enhanced risk management. Our focus should be on identifying resilient companies and sectors poised to benefit from the heightened awareness and demand for robust cybersecurity solutions.

---

Your Name

Your Position

Your Contact Information