enquire

Network Pulse Report

Question

Shares of CrowdStrike dropped more than 8% on Tuesday following news that Delta Air Lines intends to seek compensation from the cybersecurity firm for the recent global IT outage that disrupted multiple industries, including airlines. What is the likelihood that CrowdStrike will face a significant legal bill due to last week's outage? Are other companies also in a position to sue them? What are the potential implications for cybersecurity firms if they face legal repercussions after such outages or attacks? Is this a viable concern? Considering the generally positive response CrowdStrike received for its damage control and crisis management efforts, what is the outlook for the company's future?

Subject-matter Expertise

CrowdStrike, Stocks, Legal Liability, Cybersecurity, Symantec Corp.

Created Date

30 Jul 2024 11:07AM

Takeaways

- CrowdStrike faces potential legal challenges and settlements due to product failure, which could serve as a warning for other companies to improve their development and release processes.
- Technical and non- technical perspectives raise questions about CrowdStrike's protocols, security measures, upgrade processes, and audit verifications. If proven negligent, they could face significant legal bills.
- CrowdStrike's massive outage could lead to insurance claims or subrogation claims. The implications of such an event raise concerns about contract terms, indemnifications, and the future of insurance coverage for operations when patches can go wrong.
- Delta and other companies seeking compensation from CrowdStrike will likely settle out of court. The media should monitor CrowdStrike's SEC filings for disclosure of exact costs.
- CrowdStrike's 8% share drop signals potential legal action from other affected businesses. This incident highlights the risks cybersecurity companies face, including major financial losses, increased insurance costs or stricter regulations.

Answers

CTO & CISO
United States of America
30 Jul 2024, 11:16 am local

CrowdStrike will certainly face many legal challenges and will likely have to settle and pay out to at least some larger companies. It is certainly a concern for all companies, including cybersecurity ones, that they will be sued if their product fails and/or causes damages. CrowdStrike should recover because it's products are some of the best available. They will certainly need to win back the markets confidence by showing how they improve their processes. It would be naive for people to believe this is a unique situation for CrowdStrike. Hopefully, it will be a warning that others take and approve their own development and release processes.

Information Security Consultant

United States of America

30 Jul 2024, 11:42 am local

Crowdstrike will very likely face a significant legal bill due to the massive outage being attributed to a software patch as the proximate cause. Insurance companies, cybersecurity insurance, business owners insurance, loss of revenue coverage will all point to the proximate cause of the loss and either the insurance claims are paid out within policy limits or subrogation claims may even be possible. The implications for a software patching deployment going wrong are quite valid concerns as we see in the aftermath and fallout that the travel industry suffered as a result of the outage. The implications may or may not be limited or curtailed by the terms of the written contract, it depends on how legal expertise awareness existed in drafting a contract with indemnifications and hold harmless classes if any existed or will exist in the future. The concern for for cybersecurity firms is quite valid. To what extent is a contract with indemnifications and hold harmless defendable, and can business be captured with such conditions. Another cause for concern for the future is if insurance will continue offering coverage for operations when patches can go wrong.

Former FBI, CISO and Privacy & Cyber

United States of America

30 Jul 2024, 11:45 am local

Delta and many other companies will seek compensation from Crowdstrike but this will likely not be handled in open court. The master services contract that CS uses with its clients will come into play and a settlement out of court for an unknown amount either in fiat or discounted services will be reached. There will be a very significant legal bill around defending CS and in settlements. The media will need to watch CS's SEC filings about the disclosure to see the exact cost Crowdstrike has already placed the blame on a third party software checker and not their internal team in an attempt to move liability. Also the public does not understand that Delta or any of the other companies were offline because of Crowdstrike. They blame the outage on the company they directly interact with. For most Delta is solely to blame for the outage. (Even if the public knows it was a CS issue, Delta hired them so Delta is to blame) As for stock prices, CS needs to control the narrative and minimize the loss of clients. Investors will watch if companies ditch CS for another provider. Most CS contracts have a costly break clause but it might not be enough to keep clients.

Founder & CEO

United States of America

30 Jul 2024, 12:36 pm local

The likelihood of CrowdStrike facing a significant legal bill from last week's outage depends on factors like contractual obligations, incident specifics, and legal precedents. Service agreements will influence liability. Root cause and incident response are crucial. Other companies may also sue, and class- action lawsuits are possible. Mitigation includes negotiation, transparency, enhanced security, and legal preparedness. - The legal repercussions for cybersecurity firms after outages or attacks have profound implications to include financial strain from lawsuits, increased insurance premiums, reputational damage, and loss of client trust. Firms must enhance security, adjust contracts, and comply with stricter regulations. The concern is viable, and proactive risk management is essential for growth and reliability. - The outlook remains cautiously optimistic due to effective damage control, strong market position, ongoing innovation, and strategic growth initiatives. CrowdStrike's swift response maintained client trust and market confidence. Its strong reputation, diverse client base, and continuous innovation in AI and machine learning ensure relevance and growth.

Information Security Consultant

United Kingdom

30 Jul 2024, 12:42 pm local

CrowdStrike's 8% share drop signals a potential legal storm. While a direct link between the outage and CrowdStrike's products needs solid proof, Delta's claim sets an example. Other affected businesses might also take legal action, especially those with significant losses. This incident highlights the significant risks cybersecurity companies face. If found negligent, major financial losses could reduce profits and shake investor confidence. The industry could see higher insurance costs or stricter regulations, slowing down innovation. CrowdStrike's quick response lessened the impact, but rebuilding trust is difficult once it's lost. The long-term effects depend on the legal outcome, compensation claims, and the company's ability to restore confidence and prevent future issues. This event clearly shows the high- risk environment in which cybersecurity firms operate.

Software Architect

United States of America

30 Jul 2024, 12:49 pm local

Very high likelyhood that CrowdStrike will face significant legal bill due to the recent outage. While the exact terms of contracts with clients will determine the extent of their liability, some of the following factors will have a big impact: industry impact - critical ones like airlines, banking, healthcare, issue resolution turnaround, how widespread it was, financial losses, reputational damages, etc. We foresee critical infra sectors like the ones I mentioned filing lawsuits. As for implications to cybersecurity firms, this incident will result in extensive coverage and higher insurance costs, more and stricter govt regulations for higher standards and accountability, and at some extent stifling innovation and risk taking in the cybersecurity industry. Frequent lawsuits could also damage public trust in such firms making it difficult to attract and retain customers. We think CrowdStrike will bounce back even with this setback due to its quick response and transparency. They have a long, positive track record in this industry and a large and loyal customer base. The recovery will definitely be slow though and may result in immediate dip in accounts.

Director - Product Management

United States of America

30 Jul 2024, 1:41 pm local

I believe that the Crowdstrike event will have a short- term impact on its business as some customers decide to adopt a multi-vendor strategy. Thus while there will likely be lawsuits I expect that these will little effect as SaaS security firms have very strong SLAs / EULAs that limit their liability. A good example from the past to consider is Solar Winds (NYSE: SWI). They suffered a major software supply chain breach that was announced in Dec. 2020. A foreign actor (believed to be Russia) had breached SWI's build environment and for a period of 1-2 years was able to exfiltrate data from SWI's platform. SWI was a major vendor whose customers included numerous Federal agencies (including Department of Defense), global banks, and infrastructure providers. This breach was an earthquake for the industry and culminated in Executive Order 14028 on Improving the Nation's Cybersecurity. Fast forward to today (July 2024), SWI is still in business, has a market cap of $2B USD, and is growing revenue. The stock price has not recovered from the high in Dec 2020 but many companies are in a similar situation so it is hard to disaggregate the breach impact from market sentiment 3.5 years later.