KOVRR

Cyber Decisions. Financially Quantified.

The *UK Cost* of the CrowdStrike Incident

www.kovrr.com

CrowdStrike made global headlines when an automatic update to their Falcon sensor software crashed more than 8.5 million Microsoft Windows machines globally. This incident resulted in major disruption, including supermarkets being unable to take card payments, TV broadcasters going off the air, and airlines canceling thousands of flights.

This is a fascinating case because, although not a malicious attack, the repercussions mimic those of one that was. Moreover, this case demonstrates that a single point of failure, including third-party software, can cause outsized impacts. This impact is particularly significant when the specific third-party software is pervasive throughout an organization. An exacerbating feature of the CrowdStrike incident is the relatively small number of vendors dominating the market, which meant that when something went wrong, a large part of the market was affected. The common doomsday scenario has recently been an outage in a major cloud provider (Azure, GCP, AWS). Still, here we again see the potential for errors or attacks via third-party software to cripple businesses on a global scale. It seems that in many cases, the expensive lesson of SolarWinds, that unquestioningly accepting updates can be catastrophic, has not been learned. Hopefully, updates to security software will now get at least the same level of scrutiny as other software updates.

Another thought-provoking side to the CrowdStrike incident is that an anti-monopoly agreement between the European Commission and Microsoft in 2009 is one of the reasons why CrowdStrike had kernel-level access to Windows, and along with other factors, allowed it to produce the infamous blue screen of death. This instance illustrates that agreements and laws made over a decade ago can have serious unforeseen consequences and that everyone may not always understand the actual risks resulting from these decisions.

Economic Impact

Estimates of the economic impact are few and far between, but Kovrr has calculated that the total cost to the UK economy will likely fall between £1.7 and £2.3 billion ($2.18 and $2.96 billion).

This value is based upon the uptake of endpoint detection software across the market in combination with CrowdStrike's market share and assumes an average downtime of 1 working day, 24 hours. For the downtime, we know that 97% of systems have been fixed after nine days, and CrowdStrike released a fix within 20 hours. Examples show that business-critical systems were restored on varying timescales, with Sky News going off air for only a couple of hours and American Airlines grounding 400 flights on the first day and 50 flights the following day. Clearly, fixes continue much beyond 24 hours, and IT staff are still fighting to get all systems back online. However, the later fixed systems are likely to be less business-critical in the short term, so they are unlikely to contribute significantly to business interruption costs.

Kovrr's estimate considers the costs associated with business interruption, the response, and post-response expenses, such as litigation, based on Kovvr's deep understanding of system outage data from past incidents and detailed cost analysis.

To put the financial consequences of this cyber event in context, Verisk PCS estimated that NotPetya caused a global economic impact of around $10 billion (~$13 billion inflation-adjusted), and Wannacry approximately $4 billion (~$5 billion inflation-adjusted).

Many larger companies likely have cyber insurance, so they will not have to bear the total cost of this event. Moreover, because of the existence of these policies, the resulting impact on the cyber insurance market is still unfolding. Estimates of the global insured losses range from "mid to high single digit billion USD" and are unlikely to be material for the (re)insurance market. Beazley, the largest insurer of cyber risk in 2023 (6.7% of GWP), stated that the incident will not affect their profitability projections for the year.

For a broader insurance context, the 2011 Japan Earthquake (Tohoku) and tsunami produced insured losses of around $56 billion. Hurricane Katrina (2005) was the costliest natural catastrophe event and resulted in insured losses of $102 billion. The CrowdStrike event will be an interesting test of how insurance terms apply to these types of non-malicious incidents.

Definitions

Business Interruption (BI) - Loss of revenue due to interruption of normal business, e.g., production shut down, payment options shut down, and reputational damage.

Response Costs - Working out the problem, how to fix it and then fixing it. Response costs can also be expenses from internal resources or external resources brought in for the task.

Post-Response Expenses - Legal costs, regulatory costs, and other similar post-event costs.

Market Impact

The impact of the CrowdStrike event is reflected in global stock markets, showing that over the markets, the incident has had a significant impact on firms' productivity, both directly and via the complex web of supply chains that makes up the modern economy. In the UK, the FTSE 100 closed 0.6% down or approximately £21 billion, or $27 billion. Across the pond, the S&P 500 dropped 0.8%, which is a change in market cap of around $336 billion. CrowdStrike, unsurprisingly, has seen a huge impact on their share price, with a reduction of 22.9% between the 18th of July and the 24th of July, representing a change in market cap of around $19 billion. CrowdStrike is in the S&P 500 and, therefore, has directly contributed to the drop in that index.

Risk Assessment

While a malicious actor did not initiate this event, it does demonstrate again how large an impact major cyber outages can have and the impact a single provider can have across markets and portfolios. At Kovrr, we capture this through the modeling of systemic incidents, which test all companies with the same event scenarios, including a range of providers, correlating incidents across markets and geographies.

Understanding the cost to one's own company is vital, and within Kovrr's models, we actively incorporate these systemic events, as well as targeted attacks. Using our state-of-the-art model, we determine that in a given year, there is a 1 in 140 chance of an outage of this duration being caused by this kind of application.

Although systemic events have a relatively small impact on the overall risk landscape for individual entities, when it comes to understanding aggregate risk at the group level, these systemic events, malicious or not, become increasingly important.

Author:
Huw Goodall
Cyber Risk Quantifier, PhD
Kovrr