Browne Jacobson

CrowdStrike: Assessing the fallout of potentially the “largest IT outage in history”

24 July 2024

Whilst the fallout of the CrowdStrike outage is still being assessed, some IT experts are already suggesting that the events of 19 July 2024 represent the “largest IT outage in history”. This assessment seems apt, especially as at the time of writing, Microsoft has estimated that around 8.5m computers around the world were disabled by the global IT outage, which would easily make it the worst cyber event in history. This article looks at what caused the outage and considers what’s next for customers and IT vendors and suppliers.

Background

CrowdStrike is an American cybersecurity technology company based in Austin, Texas. It provides cloud workload protection and endpoint security, threat intelligence, and cyberattack response services.

On 19 July 2024, CrowdStrike released a sensor configuration update to its leading cloud-based cybersecurity platform known as Falcon. The update released by CrowdStrike triggered a logic error resulting in a system crash and blue screen on impacted systems, thereby causing a malfunction that disabled IT systems across multiple sectors worldwide.

On the same date, CrowdStrike published a manual workaround to fix the issue, however the fix does not, at present, appear to be scalable as it needs to be applied manually, system by system. With systems spread between on-premise and the cloud, it will likely take a considerable time for impacted systems to fully recover.

The incident impacted organisations using Windows machines using CrowdStrike’s software. As the software is widely used by many organisations across a variety of sectors, the outage will almost certainly have severe short-term direct and indirect impacts on the day-to-day operations of many organisations globally and low-level impacts for some time.

Legal implications

Establishing/limiting liability

As noted above, the scale of the resulting impact from the outage was enhanced by the fact that many organisations (across multiple different sectors worldwide) use Windows and CrowdStrike on their devices. Owing to the breadth of the outage it is likely that a variety of claims could be triggered, with parties seeking to recover any financial losses suffered as a result of the outage from the party next in the contractual chain. Primarily, parties will need to undertake a factual review to determine (i) how the outage specifically impacted their organisation, (ii) what accrued financial losses can be established; (iii) the impact of contractual limitation of liability provisions and (iv) whether anything could have been done to prevent / mitigate losses from arising (e.g. through efficient Business Continuity and Disaster Recovery Plans). Given the breath of the outage, the nature of the disputes that might be triggered as a result of the CrowdStrike outage will largely depend on the contractual relationships in place throughout the contractual chain (i.e., between the end user and their manged service provider and between the managed service provider and those higher up the contractual chain e.g., IT vendors (or re-sellers) such as Microsoft and CrowdStrike).

Once businesses understand the extent of the financial, operational and reputational impact of the outage (whether for themselves or their customers), consideration will then need to be given to establishing, or conversely limiting liability. IT vendors and suppliers will need to

immediately review their contracts with customers to understand the extent to which they may be shielded by a force majeure defence, or limitations and exclusions of liability. Importantly, as the cause of the outage appears unrelated to any third-party bad actors, IT vendors and suppliers might find it harder to entirely avoid liability to customers.

Conversely, customers will want to review contracts with vendors and suppliers to establish whether they are able bring claims to recover any losses that they may have suffered, although any form of breach of contract claim will likely be subject to the limitation of liability provisions in the relevant contract. Customers will also need to review contracts with their own clients who in turn might seek to bring claims as a result of the outage.

Insurance

Businesses should review their insurance policies urgently to see what cover they have in place and whether this will respond to potential liabilities that may arise. It is also advisable, at this early stage, to determine whether insurers should be notified of claims which may be made under the policies. Insurance policies commonly contain conditions, particularly in relation to notification and actions to be taken following an incident, which must be strictly complied with to preserve the claim under the policy.

Of most relevance will be cyber and business interruption policies. IT vendors and suppliers will need to determine whether they are covered for liability to customers in circumstances where there is negligence or where they are in breach of contract. Customers should also review policies to ascertain whether they are covered for loss of business income following a cyber incident, and also whether the coverage extends to an incident of this nature i.e., where there are no third-party bad actors.

Data protection

Based on the official information released so far, it appears safe to conclude that this was not a cybersecurity related incident. That being said, organisations should be vigilant to the fact that bad actors will often use the chaos of a major IT outage to gain access to systems. There have already been reports of malicious websites using the incident to publish "unofficial code" claiming to fix any ongoing issues. Organisations should therefore take care to ensure that it only relies on information published by official and trusted sources.

Further, if, during the outage, data subjects were unable to access personal data on systems, this could constitute a breach of data protection law. If any damage has resulted, organisations might be vulnerable to complaints or claims, and as such organisations should also consider whether they are required to make notifications to their data regulator.

Conclusion

As the fallout from the CrowdStrike outage continues, organisations should engage with partners, consultants, lawyers and other experts to help them navigate this unprecedented event.

If you need advice in relation to the issues discussed in this article, please contact Sophie Ashcroft or Andrew Woolsey.

Key contacts

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000

Andrew Woolsey

Associate

Andrew.Woolsey@brownejacobson.com

+44 (0)330 045 2702

Related expertise

Services

Data protection and privacy

Insurance claims defence