Perspective on the recent CrowdStrike outage: implications for insurance and cyber resilience

Insights - 02/08/2024

The commercial world was sent into a brief period of panic on 19 July when an IT outage of an unprecedented scale caused substantial disruption to businesses across the globe. We examine the potential damage caused and its impacts on cyber insurers and underwriters.

A faulty security software update pushed out by US cyber security firm, CrowdStrike, resulted in widespread outages of Windows computers, affecting a host of industries in what has been dubbed "the largest IT outage in history". Mass cancellation of flights, disruption to health services and chaos in the banking sector were among the many issues that arose from the CrowdStrike induced technical difficulties, leading to major financial losses for businesses.

Compensation and claims

With the catastrophic IT troubles now largely in the rear view mirror, this article examines the implications for the insurance sector, as affected businesses may look to claim compensation for their losses.

According to Reuters, economic damages for the disruptions could amount to billions of dollars. As a result, insurers are anticipating hundreds, if not thousands, of claim notifications.

Liability clauses

From an insurer's perspective, there is a risk that some organisations may look to their insurers for compensation. CrowdStrike appears to have comprehensively limited its liability towards users of its software with the inclusion of a limitation of liability clause in its standard terms and conditions. Liability is limited to fees paid by the user, meaning that any CrowdStrike users who were unable to negotiate out of the standard terms and conditions may be entitled to nothing more than a refund.

Larger organisations with greater weight at the negotiating table, such as the major airlines and financial institutions, may have bespoke terms and conditions with CrowdStrike which may allow them to recover against CrowdStrike. However, there is a risk that smaller commercial entities with weaker bargaining power, may look to insurers to recoup their losses.

Cyber cover

Cyber insurers and underwriters should carefully examine policy wording from a reserving perspective to assess the potential exposure from the Crowdstrike outage. As noted by Loretta Worters of the US based Insurance Information Institute, cyber policies "...typically do not cover downtime due to non-malicious cyber events at a third-party network service provider".

Business interruption cover, while not typically included in cyber policies as standard, could be one potential area of exposure for insurers depending on policy wording. Cyber insurers should review policies for any such exposure and risk assess for potential claims arising from circumstances such as those which arose from the CrowdStrike outage.

The Digital Operational Resilience Act (DORA)

In a recent article we outlined how companies can prepare for cyber security incident such as the Crowdstrike outage, following the introduction of the Digital Operational Resilience Act (**DORA**). The CrowdStrike outage further emphasises the importance for businesses to take steps to identify potential risks, carry out testing to draw out IT vulnerabilities and strengthen their operational resilience, as mandated for in-scope entities by DORA.

More than 22,000 financial entities across the EU are estimated to be subject to DORA, including credit institutions, banks, insurance/reinsurance undertakings, investment firms and payment institutions. The events of 19 July 2024 exposed a weakness in the global IT landscape, and perhaps an over-reliance on IT infrastructure by some organisations, without the necessary backups being in place for adequate protection. Adherence with DORA by in-scope entities and the taking of necessary steps towards compliance can ensure that businesses are better equipped to deal with such types of outages in the future.

What's next for cyber disruption?

The insurance coverage position arising out of the CrowdStrike disruption will be watched with keen eyes over the coming months. As put by Cyberwrite CEO Nir Perry, this incident was "an event that will be referred to in the years to come when assessing risk". Insurers and underwriters should take the opportunity to risk assess their policies and potential exposure, as it is inevitable that similar large scale outages will reoccur in future – in what shape or form remains to be seen. For more information about cyber matters please contact a member of our team via their contact

details below.

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

This client briefing has been prepared for clients and professional associates of Ogier. The information and expressions of opinion which it contains are not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific advice concerning individual situations.

Regulatory information can be found under Legal Notice

Key Contacts

Cian O'Gorman

Associate

Ireland

E: cian.o'gorman@ogier.com

T: +353 1 584 6766

Stephen O'Connor

Partner

Ireland

E: stephen.oconnor@ogier.com

T: +353 1 232 1074

Matthew Shaxson

Group Partner, Ogier Legal L.P.

Jersey

E: matthew.shaxson@ogier.com

T: +44 1534 514064

Richard Sharp

Partner

Guernsey

E: richard.sharp@ogier.com

T: +44 1481 752257

Cathal Keane

Trainee Solicitor

Ireland

E: cathal.keane@ogier.com

T: +353 1 584 6308

Related Services

Insurance and Reinsurance

Related Sectors

Technology and Web3