FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

APRIL 2025

Key takeaways from the CrowdStrike event survey

This information sheet provides a summary of the results from a survey conducted in October 2024 to provide a snapshot of the preparedness and responsiveness of financial service providers that were impacted by the CrowdStrike incident.

One of the statutory objectives of the Financial Markets Authority – Te Mana Tātai Hokohoko (FMA) is to promote the confident and informed participation of consumers, investors, and businesses in the financial markets. The operational resilience of financial service providers is critical for supporting the integrity of New Zealand's financial markets and encouraging confident participation.

On 19 July 2024, a problematic security software update released by cybersecurity company CrowdStrike impacted Windows operating systems and caused widespread global IT outages.

Many financial service providers we license are required to notify us of any incidents that materially affect the continued provision of their market service. However, we received a low number of notifications following the CrowdStrike incident. To better understand the impact, we asked selected licensed entities to complete a voluntary survey.

We are sharing the findings from this survey to encourage financial service providers to thoroughly assess and update their business continuity plans (BCP) and emergency procedures, irrespective of the impact the CrowdStrike event may have had on customers, critical technology systems or third-party providers.

Note that all findings are based solely on the survey results, and all responses were anonymous. We would like to thank everyone who participated in this survey. If you have any further questions, please email questions@fma.govt.nz.

Findings

Number of notifications

Approximately 23% of the 66 survey respondents indicated they were impacted by the CrowdStrike incident. Of this proportion, around 70% reported they did not notify the FMA, believing the incident did not materially impact their critical technology systems, or their customers. Some respondents indicated that extensive media coverage of the CrowdStrike incident influenced their decision not to notify the FMA.

Financial service providers that are required to notify the FMA of any event that materially impacts the information security or operational resilience of their critical technology systems must ensure such notifications are made promptly and within the timeframe required by their licence obligations[1].

Ability to respond to disruptive events

Around 70% of impacted respondents activated their internal incident response processes as a result of the CrowdStrike incident. The majority rated their response processes either “Very good” or “Excellent”.

Respondents were also asked to rate their ability to respond to a disruptive event before, during, and after the CrowdStrike event. The percentage of respondents who rated their ability to respond to a disruptive event as “Very good” and “Excellent” increased from around 50% before the incident to 70% after the incident. Many respondents shared how the CrowdStrike incident helped identify and remediate gaps in critical functions such as communication, stakeholder management, and technology systems. This may indicate that such disruptions can serve as valuable opportunities for financial service providers to reflect on lessons learnt.

We encourage financial service providers to conduct post-incident reviews, incorporate crisis simulations and conduct case study walkthroughs as part of their BCP testing procedures. Financial service providers should also review whether their current testing procedures are appropriate for the scale and complexity of their business, and if their software systems require any update or enhancements to improve operational resilience. We also encourage all financial service providers to seek professional advice and guidance to ensure BCP and emergency protocols are robust and appropriately tailored to the unique scale and complexity of their business.

Impact on customer base

Of the entities surveyed that stated they were impacted by the CrowdStrike outage, around half indicated their customer base was also affected. Of these entities, most respondents rated their ability to alleviate customer impact as “Very good”. Many noted they were able to minimise customer impact through timely communication of transparent information. Some explained they had an alternative workflow, and/or enhanced their customer support by temporarily increasing capacity. Most entities also rated their ability to address customer impact for similar events in the future as “Very good”. Respondents noted the importance of effective communication with both internal and external stakeholders when managing the CrowdStrike event, and some identified gaps in their internal communication processes. By developing robust communication streams that provide timely updates during disruptive events, financial service providers can better manage market expectations, build customer trust, and minimise reputational risks.

Impact on third-party providers

Over 70% of respondents use third-party providers in the provision of their financial services. Approximately 30% of these providers were impacted by the CrowdStrike outage. Overall, survey participants indicated they were largely satisfied with their third-party service providers’ responses to the incident, and their ability

[1] More information relating to business continuity and technology systems for entities can be found here

to respond to similar events in the future. The outsourced functions most affected by the CrowdStrike event were transaction and payment processing, application and operational tasks, IT services, and call centre operations. The most common way respondents discovered that their third-party provider was affected by the CrowdStrike event was via direct notification from the provider, followed by updates from their internal IT team, information from staff members, and system outage notifications. Most respondents appeared to have procedures in place to receive notifications directly from third-party providers of any material impacts on their critical technology systems.

However, approximately 10% of respondents who indicated they use third-party providers in the provision of their financial services were unsure whether the CrowdStrike incident had a material impact on their third-party provider. We encourage all financial service providers to have sufficient oversight over their third-party providers and all outsourcing arrangements. Financial service providers subject to standard licence conditions for outsourcing arrangements must ensure their providers can adequately deliver and perform their services to the standard required for the licensee to fulfil their market service obligations[2].

Licensed financial advice providers, discretionary investment management service (DIMS) providers, managed investment scheme (MIS) managers, Derivative Issuers (DI), Peer-to-peer lending, Crowdfunding service providers, and all financial institutions under the Conduct of Financial Institutions (CoFI) regime are all subject to a standard licence condition relating to business continuity and technology systems. This requires them to have and maintain an appropriate business continuity plan, and to report to the FMA any events that materially affects the continued provision of their market service. All licensees should be familiar with the specific obligations of their licence type and have systems in place to ensure compliance.

We encourage anyone who provides a financial service – not just licensees – to review our resources on operational resilience. This information will help you to consider what plans or processes you need to put in place or improve, to ensure you can continue to deliver critical operations through disruptions.

[2] More information relating to business continuity and technology systems for entities can be found here