Crowdstrike: important takeaways for customers and suppliers

On 19 July 2024, cybersecurity firm CrowdStrike experienced a significant service disruption that affected many of its customers globally, including banks, airlines, and healthcare providers. The incident highlighted the dependence of businesses on cloud based IT systems and raised concerns about the resilience of even the most robust platforms. In this article we outline some important takeaways for both customers and suppliers of cloud based systems.

The incident

The disruption began in the early hours of Friday morning. CrowdStrike pushed a sensor configuration update for Windows that caused an error, resulting in the infamous 'blue screen of death' (BSOD). Any computer that was online and running the Falcon sensor for Windows v.7.11 or newer was at risk when the Windows devices automatically updated.

CrowdStrike promptly acknowledged the issue through their official status page and social media, and worked quickly to identify the root cause of the problem, isolate the fault, and began the process of rectifying the errors.

The service disruption had a varied impact on customers. Some reported minor inconveniences, while others, who were relying on CrowdStrike's real-time threat detection and response capabilities, faced significant operational challenges.

The incident provides important learning points for both customers and suppliers.

Lessons for customers

For customers, the incident underscores the importance of having contingency plans in place for failures of cybersecurity services, as any lapse can leave them vulnerable to attacks. It also demonstrates the operational impact of IT systems being unexpectedly offline, even for short periods.

The importance of business continuity

Perhaps one of the most striking aspects of the incident is the ability of the failure of one cybersecurity product to bring down computer networks around the world, and the apparent lack of robust business continuity plans which should have been in place to enable affected businesses to continue their operations with limited disruption.

End-users might have expected banks, airlines, hospitals and internationally recognised businesses to have proactively planned and prepared for IT system failures to ensure the organisation could continue operations with minimum impact to customers and clients. But many appeared to be incapacitated by the incident.

A key feature which appeared to be lacking was meaningful failover. In the IT context, failover is a component of business continuity which involves switching to a redundant or standby system upon the failure of the primary system. Failover mechanisms are intended to ensure that if a primary IT system fails, business operations can continue with minimal interruption by automatically or manually transferring tasks to a backup system.

Continuity plans

The CrowdStrike incident highlights the need for businesses to review their business continuity plans. These plans should include:

1. Risk Assessments and Business Impact Analysis: This is the first step in planning and it involves identifying potential risks and assessing their impact on business operations. Reliance of IT systems should be picked up as a key risk factor in any business impact analysis.
2. Developing a Business Continuity Plan (BCP): A BCP outlines the procedures an organisation must follow in the face of disaster. The BCP should include detailed information on recovery strategies for IT systems, such as alternative communication channels and data recovery.
3. Failover Mechanisms: This involves implementing secondary systems that can take over in the event of a failure of the primary systems.
4. Data Backup and Recovery: Regularly data backups are essential. Organisations should implement automated backup systems and ensure that backups are stored securely on separate systems so they don't become inaccessible in the event of a failure of the primary system.
5. Testing and Training: Regular testing of BCPs is crucial to ensure they work effectively. This includes running simulations and drills to train employees and identify potential weaknesses in the plans.

Diversification and reducing over-reliance

As evidenced by the CrowdStrike incident, the over-reliance on a narrow set of IT systems presents significant risks that can jeopardise an organisation's functionality and resilience and can result in the creation of a single point of failure. If a business is heavily reliant on a few key systems, any disruption (whether due to technical malfunctions, cyber-attacks, or human error) can lead to operational paralysis.

A narrow IT system portfolio can also increase cybersecurity vulnerabilities and, if an organisation does not diversify its IT infrastructure, it may not have adequate backup systems or contingency plans, making it more

challenging to recover from an attack.

Also, while not crucial to a business's day-to-day operations, over-reliance on a narrow set of IT systems can stifle innovation and lead to operational rigidity which can hinder its ability to adapt to changing market conditions and make it harder to stay competitive.

To mitigate the risks associated with over-reliance on a narrow set of IT systems, businesses should pursue strategic diversification, adopting a multi-vendor approach, a range of technologies, and regularly updating systems to keep pace with technological advancements. Strategic diversification shouldn't be limited to using different software and hardware solutions but should also extend to fostering a culture of innovation and adaptability.

Lessons for suppliers

For suppliers, the CrowdStrike incident highlights three key takeaways:

Pre-release testing

For IT suppliers it is vitally important to maintain robust mechanisms for pre-release testing and validation before updates are pushed live. This shouldn't simply be seen as a tick-box in the development process; it's an essential practice that ensures the delivery of high-quality, reliable, and secure software.

Pre-release testing should include multiple steps and validation checks to allow developers to identify and fix bugs before the code is released. This enables them to catch issues early, and to address them when they are easier and less expensive to fix. It also avoids the fallout which results from problematic code being released to customers and end-users.

Pre-release testing isn't just about finding bugs; it's also about ensuring that the software performs well under various conditions. Performance testing can reveal bottlenecks, memory leaks, and other issues that could degrade the user experience. Optimising performance before release ensures that the software can handle real-world usage effectively and avoids poor end-user experiences which can negatively affect the supplier's reputation

Detection and monitoring

Whilst pre-release testing should capture the most significant of errors, mistakes will still occur. For this reason, a good quality assurance process should also include post release detection and monitoring to ensure code releases are stable and reliable and don't negatively affect system performance.

This detection and monitoring could involve a variety of strategies, including log analysis, performance metrics, error tracking, and user feedback collection. Real-time monitoring tools can also be used provide insights into how the release affects system performance, identifying issues such as increased response times, memory leaks, or higher error rates and providing automatic alerts to the supplier to enable them to take steps to mitigate potential problems swiftly.

Reputation management

Although the latest incident resulted in a dramatic drop in CrowdStrike's share price and is an incident it will no doubt have preferred to avoid, some industry professionals have praised CrowdStrike for how quickly and effectively it managed the situation and have pointed out that the transparency shown by CrowdStrike during the incident may in fact help to build customer trust in the long term.

For other suppliers this incident highlights the importance of strong reputation management. An IT system failure, particularly one that disrupts services or compromises data, can severely damage a company's reputation if not handled properly. Effective reputation management involves a combination of transparent communication, swift action, and strategic long-term measures.

As demonstrated by CrowdStrike, open and honest communication with affected parties can not only reduce the impact of the IT incident itself, it can also help to mitigate frustration and build trust. The communication should include what happened, the extent of the impact, and steps being taken to resolve the issue. Timely updates are also essential to keep everyone informed and to show that the company is actively addressing the problem.

Now that the immediate crisis has been handled, CrowdStrike will no doubt be conducting a thorough post-mortem analysis to understand what went wrong and will be implementing improvements, and both short-term and longer-term strategies, to avoid future incidents.

Conclusion

It is yet to be seen what the long-term business impact will be for CrowdStrike, but the incident provides some useful takeaways. IT service suppliers should take this as a warning and use the opportunity to carry out a review of their processes. They should ensure they have rigorous testing and validation procedures for network updates before they are made live and should ensure they have suitable monitoring systems in place to detect potential issues and should handle potentially damaging reputational implications before they escalate.

For their customers, this incident is a reminder of the importance of resilience and preparedness in relation to their business continuity strategies. They should also revisit their reliance on single-point solutions and consider incorporating redundancies and diversifications into their approach.

Kathryn Rogers

Partner