KPMG

Navigating the fallout

Lessons from the CrowdStrike outage

July 2024

In an era where technology underpins nearly every aspect of business operations, the resilience of IT systems to withstand sudden disruptions is vital. Friday's IT outage triggered by an automatic software update deployed by cybersecurity company CrowdStrike underscores the fragility of these systems.

Global disruption

The code that temporarily froze global financial, healthcare, 911, transportation, and business operations was reportedly not the result of a cybersecurity breach. Ironically, the widespread outage was caused by a software patch intended to detect and analyze threats.

Numerous public and private sector organizations that use the ubiquitous Microsoft Windows operating system experienced an IT disruption on Friday. In the early hours — starting in Australia and working steadily westward — a faulty software update from cybersecurity firm CrowdStrike caused Windows-based computers to continually crash.

Although CrowdStrike has publicly stated that the issue was not related to a cyberattack, which is reassuring, its impact on global IT systems is significant, revealing critical lessons for enterprises around preparedness and response strategies.

And it has many companies re-examining their third-party partners' software development lifecycle (SDLC) processes and their own business continuity plans.

The incident unpacked

In this instance CrowdStrike released a defective update to their Falcon sensor security software for Windows. For thousands of computers at many organizations this initiated a loop of the infamous Windows "blue screen of death," a system crash indicator.

The oversimplified fix is to boot the infected machine into Safe mode, delete the bad file and reboot. The obstacle is that most current Microsoft systems are encrypted with BitLocker, which requires a recovery key (if you are unfamiliar with a BitLocker key, it is an exceedingly long string of characters).

As a result, IT admins globally were forced to go from server-to-server—and in some cases, physically from desk-to-desk—with USB drives containing BitLocker keys to manually get these systems back up and running. This is a painstaking, very manual process. It's time-consuming to go endpoint-by-endpoint to restart each affected system.

This was not simply a technical glitch. It was a wake-up call for organizations worldwide about the importance of strong and stable SDLC protocols and the need for thorough business continuity planning.

Backup and recovery planning

As many organizations continue to work to restore operations the incident further highlights the criticality of maintaining a responsive and efficient backup and recovery strategy to mitigate the impact of such outages. This includes evaluating the ability to handle recovery at scale and under pressure.

In this context, we would highlight seven key action steps:

1. **Develop a backup and recovery strategy that is scaled to your organization.**
2. **Do regular testing of your backup and recovery strategy to make sure it is properly maintained and up to date.**
3. **Assess your capacity to execute your strategy at scale based on your targeted recovery objectives.**
4. **Incorporate loss-of-access scenarios into your disaster recovery planning, including situations where physical access may be required, as well as loss-of-enterprise network access for cloud and third-party hosted environments.**
5. **Conduct regular impact assessments to better understand the blast radius if a specific service or app fails or the network is breached.**
6. **Review your software vendor list and other critical third parties to avoid an over dependence or over concentration on one or a small number of suppliers and perform regular assessments of the controls at critical third parties.**
7. **Review insurance policies in relation to third-party outages to determine whether financial impact can be reduced through coverage in business interruption insurance.**

The importance of third-party risk management

The CrowdStrike outage serves as a stark reminder of the need for diligence in selecting and monitoring third-party vendors, especially those critical to IT infrastructure.

In this case, a breakdown in the SDLC and change management process at CrowdStrike resulted in cascading outages across the globe. Using vendors with rigorous SDLC and change management processes is not optional — it is a necessity.

Businesses need to intensify their scrutiny of third-party vendors' practices. Specifically, businesses are encouraged to enhance their programs to include:

Routine risk assessment

Maintain a broad inventory and perform a risk assessment of third parties involved in the delivery of business software and services to assess their operational viability, financial health, security practices, compliance history, and previous incidents.

Contractual protections

Define clear SLAs that outline performance expectations, uptime requirements, and penalties for non-compliance.

Regular auditing and monitoring

Perform regular reviews of the controls in place at third parties including periodic audits, reviews of SOC1/SOC2s, and ongoing dialogue with critical vendors to proactively address issues and concerns. Particularly important are the software update and certification processes — requesting that vendors conduct thorough testing and validation before deploying updates is crucial.

The importance of third-party risk management

The CrowdStrike outage serves as a stark reminder of the need for diligence in selecting and monitoring third-party vendors, especially those critical to IT infrastructure.

In this case, a breakdown in the SDLC and change management process at CrowdStrike resulted in cascading outages across the globe. Using vendors with rigorous SDLC and change management processes is not optional — it is a necessity.

Businesses need to intensify their scrutiny of third-party vendors' practices. Specifically, businesses are encouraged to enhance their programs to include:

Resilience and contingency planning

Beyond immediate technical fixes, organizations should cultivate a culture of resilience, embedding robust contingency plans that encompass not just IT infrastructure but also key business operations.

Resilience doesn't mean there will never be another incident — there likely will be. It means being better equipped to manage future incidents quickly, efficiently, and with limited business impact.

Organizations can't control external threats, but they can control their own preparedness.

In conclusion

The CrowdStrike outage is a compelling reminder of the interconnected nature of modern IT ecosystems and the cascading effects a single point of failure can have across global operations.

As businesses continue to navigate the digital age, investing in resilient infrastructure, rigorous third-party risk management, and wide-ranging, coordinated recovery plans is not just prudent but essential. In doing so, organizations can more effectively shield themselves from the fallout of future incidents and improve their ability to maintain continuity in the face of unforeseen challenges.

How KPMG can help

Smart businesses don't just manage risk, they use it as a source of growth and competitive edge. Technology makes many things possible, but what's possible isn't always safe. We can help you create a resilient and trusted digital environment in the face of evolving vulnerabilities and threats. Specifically, we can:

Our professionals bring a combination of technological expertise, deep business knowledge, creativity, and a passion to protect and progress your business. We are available to help you protect and optimize your digital environment.

Review and test your Business Continuity and Data Recovery plans (BCP/DR)

Review and test your cyber resiliency strategy

Review your third-party risk management and supply chain management strategy

Add scale and assist with CrowdStrike remediation for this current outage

Add burst capacity through a technology and cyber recovery retainer to improve your ability to manage and mitigate future incidents

Contacts

Ton Diemont
Partner, Head of Cybersecurity & Privacy
KPMG Saudi Levant
E: antondiemont@kpmg.com

Robert Martin
Partner, Cybersecurity & Privacy: Cyber Defense & Response
KPMG Saudi Levant
E: robertmartin3@kpmg.com

Tarek Okasha
Partner, Digital Trust & Resilience
KPMG Saudi Levant
E: tokasha@kpmg.com

Timothy Wood
Partner, Cybersecurity
KPMG Lower Gulf
E: timothywood@kpmg.com

Dimitri Petropoulos
Partner, Cybersecurity
KPMG Lower Gulf
E: dpetropoulos1@kpmg.com

Tejas Ajitkumar Mehta
Partner, Governance Risk & Compliance Services & Tech Risk
KPMG Lower Gulf
E: tmehta4@kpmg.com

Fahad Alduraibi
Principal, Cybersecurity & Privacy: Cyber Defense & Response
KPMG Saudi Levant
E: falduraibi@kpmg.com

kpmg.com/sa