CrowdStrike: CRC Member Insights

On July 19, 2024, CrowdStrike, a leading cybersecurity company, experienced a significant incident where a faulty content update for their Falcon sensor security software caused widespread system crashes and disruptions. The issue primarily affected Windows hosts and resulted in service outages, particularly impacting airports and other critical infrastructure. While CrowdStrike promptly addressed the problem and provided remediation tools, the incident raised concerns about transparency and communication, prompting discussions among industry professionals about the need for stronger vendor accountability and improved incident response protocols.

CyberRisk Collaborative

The **CyberRisk Collaborative** convened a Rapid Action Meeting to allow members a forum to discuss the incident, share information, and obtain advice from fellow members. The meeting, held virtually, brought together CISOs and senior leaders from various industries and sectors to share experiences, lessons learned, and best practices for recovery and mitigation. These meetings are a primary benefit of membership in the CyberRisk Collaborative.

A poll conducted during the meeting revealed that most affected organizations were able to recover their systems within hours of the incident. However, the impact was more severe for organizations relying on cloud-based operating systems, as block-level backups made the recovery process more challenging. Additionally, organizations with decentralized IT operations faced a deluge of help desk calls, further straining their resources.

Participants shared their experiences and insights during the meeting, highlighting the importance of:

Incident Response Planning	Having a well-defined incident response plan in place proved crucial for quick identification and isolation of the issue. Organizations with established procedures were able to respond more effectively and minimize downtime.
Communication and Collaboration	Open communication channels between IT teams, security teams, and executive leadership facilitated rapid decision-making and coordinated response efforts. Regular updates to stakeholders ensured transparency and minimized confusion.
Backup and Recovery Strategies	Organizations with comprehensive backup and recovery strategies were better equipped to restore their systems swiftly. The incident underscored the importance of regularly testing backups and having multiple recovery options available.
Vendor Support and Transparency	While CrowdStrike provided remediation tools, many CISOs expressed a desire for greater transparency regarding the root cause of the incident, how distribution channels were bypassed, and what measures CrowdStrike will take to prevent future issues. This highlights the importance of clear and open communication between vendors and customers during critical incidents.
Continuous Improvement	Participants emphasized the need for continuous improvement of incident response plans and security measures. Regular review and updates of procedures can help organizations adapt to evolving threats and minimize the impact of future incidents.

Lessons Learned from the CrowdStrike Incident

- Incident Response Planning is Key
- Backup and Recovery Strategies Need to Be Improved
- Vendor Support and Transparency Goes a Long Way
- Continuous Improvement Can Be Found in Every Incident
- Cloud-Based Systems Posed Unique and Unaddressed Challenges
- Decentralized IT Can Cause Strain During an Incident
- The Value of Industry Collaboration Can Not be Overstated

Despite the frustrations regarding CrowdStrike's transparency, most participants expressed that they would likely not remove CrowdStrike as a vendor, recognizing the value of the company's security solutions and their overall track record. The CyberRisk Collaborative's Rapid Action Meeting served as a valuable forum for information sharing and collaboration. The lessons learned from the CrowdStrike incident will help organizations enhance their cyber resilience and prepare for future challenges. The collaborative effort demonstrated the power of collective knowledge and the importance of a unified approach to cybersecurity, as well as the need for ongoing dialogue between vendors and customers to ensure trust and transparency.