Armstrong Teasdale

August 26, 2024 • Advisory • www.atllp.com

THREE ORGANIZATIONAL BEST PRACTICES HIGHLIGHTED BY THE CROWDSTRIKE INCIDENT

From flight cancellations to malfunctioning hospital systems and everything in between, it would be next to impossible to find an organization that was not impacted by the CrowdStrike outage incident that took place on July 19, 2024. CrowdStrike, a Texas-based cybersecurity company, released a faulty software update to its security software used on Microsoft Windows computers which caused approximately 8.5 million systems throughout the world to crash in what is believed to be the largest systems outage in information technology history.

The CrowdStrike outage incident underscores the importance of three key takeaways: 1) internal policies and procedures should strive to prevent outages; 2) solid vendor contracts are crucial for managing risk and clarifying roles; and 3) incident response and business continuity plans should address vendor vulnerabilities.

1. INTERNAL POLICIES AND PROCEDURES SHOULD STRIVE TO PREVENT OUTAGES

The CrowdStrike incident highlighted the difficulty organizations face when critical vendors experience outages or incidents. Because it is not always an option to pivot away from using certain vendors that are critical to the organization's operations, mission or infrastructure, organizations instead must be prepared to address and remediate issues when they arise. There are several policies and procedures that organizations should implement to address and prevent a similar outage from causing major disruptions to their business practices:

- **Business continuity plan**: identify the systems, vendors and tools the organization relies upon to operate. Determine the criticality of the system, vendor, or tool, and the potential impact to the organization if the system, vendor, or tool is unavailable to the organization for various intervals, ranging from a few minutes to several days in the event of a zero-day scenario that requires extensive fixing. Prepare for the worst and develop a backup plan for operations if the tool, system, or vendor is unavailable.
- **Effective patch management**: test patches in a controlled environment before fully deploying a software update to prevent the introduction of

PEOPLE
Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES
Data Innovation, Security and Privacy
Technology Transactions

issues into the broader system. When your organization relies on a third-party vendor or organization to provide a patch or update, develop a system to ensure your organization is notified or aware of all patches and updates, including a schedule for implementation based on the criticality of the patch or update.

- **Security safeguards**: implement recommended security safeguards and practices – such as network segmentation and access controls – to reduce the introduction of faulty software at the system level.
- **Adequate employee training**: train and prepare employees at all levels to identify and address software-related issues, which can assist with avoiding critical outages. Train employees how to react to systems outages, including steps they should and should not take in the event of an outage.

2. SOLID VENDOR CONTRACTS ARE CRUCIAL FOR MANAGING RISK AND CLARIFYING ROLES

Although CrowdStrike has been proactive in rectifying the outage, not all software vendors are willing to provide remedies to their customers without a formal obligation to do so. Many software agreements provide customers with the option to terminate the contract in the event of an outage, but this remedy does not help organizations pick up the pieces when an outage leads to major financial and operational losses. Ideally, software agreements should specify the parties' responsibilities in the event of outages, including whether all parties have responsibilities, and should further specify what those responsibilities are, as applicable.

3. INCIDENT RESPONSE PLANS SHOULD ADDRESS VENDOR VULNERABILITIES

Due to the sheer amount and different types of software used by organizations, not all outages can be avoided. It is imperative that organizations implement incident response plans, including Business Continuity and Disaster Recovery (BC/DR) measures, to mitigate the impact of faulty software updates on an organization's operations.

The CrowdStrike outage has revealed just how vulnerable organizational systems can be in the event of a faulty software update. The above three considerations are proactive and preventive risk mitigation techniques that organizations can adopt to be more prepared if and when a similar outage occurs. Our Data Innovation, Security and Privacy lawyers can assist you with determining how your business operations may be impacted by cyber events and with crafting tailored compliance solutions. For more information specific to your business needs, please contact one of the listed authors or your regular Armstrong Teasdale lawyer.

Armstrong Teasdale