# Narrative of the Event and Key Learnings from CrowdStrike Incident

## Narrative of the Event

On July 18, 2024, our organization, along with many others globally, experienced a significant disruption due to a faulty update in CrowdStrike's Falcon Sensor software. This update, which was automatically pushed to many systems, caused Windows machines to crash, resulting in the infamous 'Blue Screen of Death' (BSOD). As a large retailer, this incident potentially affected our point-of-sale systems, inventory management, and customer service operations, causing disruptions in our ability to serve customers effectively

While we acknowledge the impact has been significant and widespread to our customers, we want to assure our customers that the management and teams are employing significant focus and resources to address the situation and return back to normalcy at the earliest. In addition to the short term measures being deployed to contain and course correct the situation, the following steps are being taken, to avoid such unfortunate incidents from occurring in the future:

## Key Learnings and Future Strategies

### Update Management

**What Happened:** Automatic updates led to widespread system failures.

**Future Strategy:** Implement a staged rollout process for all critical software updates. Begin with non-critical systems and gradually expand to ensure stability before full deployment.

**Production Deployment process**

**Outcome:** The changes were propagated to the production environments directly, without a proper vetting mechanism of the deployment and a safety net in place to contain the potential impact to the downstream applications.

**Future Recommendation:** We would establish a staging/pre-production environment, identical to the production environment. All the proposed production changes would be deployed to this environment first, verified, and then be propagated to the necessary production environments in a controlled and contained manner. Appropriate post production deployment validation procedures, would be established to ensure a successful deployment.

**Future recommendation:** Revisit and enhance the existing quality gates, system and management authorizations, and other checks/balances in place, to prevent third party applications from making unauthorized system changes to our production systems directly. Proposed system changes must be verifiable (and be rolled back if required) at every quality gate, in the deployment lifecycle.

**Change Control Procedures**

**Outcome:** The changes to our production systems originated from a third party application, and our teams were not aware of what those changes were

**Future recommendation:** Revisit and enhance the existing change control procedures to understand the nature of the changes being deployed, their impact and potential risks associated with the deployment. A suitable deployment strategy would be implemented for such changes, so as to minimize system disruptions

**Future recommendation:** Conduct an impact analysis of the proposed changes, on the downstream applications and perform the necessary system enhancements, testing, verification, user training, and stakeholder communication at appropriate levels.

### Testing Procedures

**What Happened:** The faulty update wasn't caught before widespread deployment.

**Future Strategy:** Enhance our testing environment to mirror our production setup more closely. All updates, especially for critical security software, should undergo rigorous testing in this environment before any production deployment.

Appropriate system and management approvals must be obtained before the changes are propagated into production.

### Rollback Capabilities

**What Happened:** Many systems were left inoperable without an easy rollback option.

**Future Strategy:** Develop and maintain robust rollback procedures for all critical systems. This includes creating system restore points, maintaining easily accessible backups, and implementing automated rollback scripts that can be triggered remotely.

### Redundancy and Business Continuity

**What Happened:** The widespread nature of the issue left many organizations without operational systems.

**Future Strategy:** Implement redundant systems running on different update schedules. This ensures that if one system fails due to an update, we can quickly switch to a backup, minimizing downtime.

From a medium term perspective, look at establishing a mirrored Redundant Production environment to minimize disruptions and ensure business continuity in case of such catastrophes.

### Vendor Management

**What Happened:** Organizations were dependent on CrowdStrike for information and solutions.

**Future Strategy:** Establish and maintain direct lines of communication with critical software vendors. Regularly review and update our vendor assessment processes, focusing on their update procedures and incident response capabilities.

Revisit existing service and operational level agreements and implement tighter standards (contractually as well as operationally) to prevent such situations from occurring in the future

### Incident Response Plan

**What Happened:** Many organizations were caught off-guard by the scale and nature of the incident.

**Future Strategy:** Develop and regularly practice an incident response plan specifically for update-related failures. This should include clear communication protocols, both internal and external, and defined roles and responsibilities for rapid response.

Also implement industry best practices around service and incident management to provide accurate and timely stakeholder communication around the resolution of such incidents.

### Monitoring and Early Detection

**What Happened:** The issue spread rapidly before it could be contained.

**Future Strategy:** Enhance our monitoring systems to quickly detect anomalies post-update. Implement automated systems that can halt further update deployments if problems are detected.

### Employee Training and Awareness

**What Happened:** Staff may have been unprepared to handle such a widespread system failure.

**Future Strategy:** Conduct regular training sessions for IT staff and key personnel on handling critical system failures. Ensure all employees are aware of basic procedures during IT outages.

## Conclusion

The CrowdStrike incident serves as a crucial reminder of the delicate balance between security updates and system stability. As a large retailer, our ability to quickly adapt and respond to such incidents is paramount. By implementing these strategies, we can significantly enhance our resilience to similar events in the future, ensuring minimal disruption to our operations and maintaining our commitment to customer service excellence.

Moving forward, let's prioritize the implementation of these learnings, starting with our update management processes and testing procedures. We'll schedule regular reviews of our incident response plans and conduct drills to ensure we're always prepared for the unexpected.

We will also ensure that through the implementation of these remediation steps, we would neither cause delays in our ability to respond to changes, nor cause unnecessary customer disruptions, while continuing to keep the quality of our customer service, as our utmost priority.