

Subject: Urgent: Critical IT Incident Notification Caused by failed CrowdStrike release
To: [CEO's Name]

Date: July 19, 2024

Dear [CEO's Name],

I am writing to inform you about a critical IT incident that occurred on July 18 at 10:20PM PST caused by one of our software vendors CrowdStrike. Note CrowdStrike is one of the most popular Endpoint Detection & Response Software providers (i.e. Antivirus) used by companies today. Here are the details:

Incident Overview:

- **Incident Description:** We have received widespread reports of Windows machines encountering significant availability issues because of a failed software update by CrowdStrike. This is not a cyber attack, this is an IT outage.
- **Impact:** This IT incident caused many IT organizations to encounter a state where their Windows Machines became inoperable (Commonly known as a Blue Screen of Death). This fix requires a manual reboot method which has proven difficult to deploy at scale. Systems that have already encountered this failed inoperable state may be down for a number of days before the IT help desk can perform an onsite visit to troubleshoot the affected machine. As a response to this issue many IT organizations disabled or turned off their Windows machines to minimize any harm until CrowdStrike could release a fix.
 - For example: Numerous airlines have stopped flights to prevent harm that could come from windows machines being unavailable during flight activities.

Immediate Actions Taken:

- **List of Actions Taken:** We are following the official guidance from the CrowdStrike Customer Support Portal. This portal recommended organizations reboot Windows machines into a Safe mode so that the file causing the issue can be deleted.
 - We are performing this recommended step so that Windows machines can be rebooted without any future harm.
 - Additionally we are deploying the newest fix by CrowdStrike to prevent this harmful release from having any more negative impact on our organization.
- Given the requirement for the IT to support numerous machines, we anticipate that there will need to be a large prioritization effort to troubleshoot effectively.

- Note the requirements for your machine to be in scope of this incident is your machine must be running both Microsoft Windows and CrowdStrike. Thus if you run an Apple Macbook or non-Windows Server, then you are not affected by this incident.

Current Status:

- The CEO of CrowdStrike has acknowledged the issue and has identified this was not a security incident or cyberattack. They are referring customers to the support portal for the latest updates. CrowdStrike has issued a fix which most organizations are deploying at this time.

Estimated Time to Resolution:

- We expect to have all systems fully operational by [Date and Time]

Further Communication:

- **Bottom Line:**
 - We anticipate Windows machines may be down for a number of days.
 - We will also be asking for clarification from the business units on prioritization of assets
 - We anticipate company-wide emails to be sent to keep folks informed and productive while they work from their mobile devices.
 - We are redirecting IT/cyber personnel in a temporary response to prioritize remediation of this incident.
- **Next Update:** [Provide details on when the next update will be provided, e.g., "We will provide the next update at [Time]."]
- **Contact Information:** [Provide contact details for further inquiries, e.g., "For any urgent questions, please contact [Your Name] at [Your Phone Number] or [Your Email Address]."]
- **Root Cause Analysis:** [Note failed software releases can happen to any organization. We will be performing a root cause analysis on this incident to identify if there are any future steps we could take to prevent this event from happening again. We will provide the details of this Root Cause Analysis on ...]

We understand the critical nature of this incident and are working diligently to resolve it as quickly as possible. Thank you for your patience and understanding.

Sincerely,

[Your Name]

[Your Title]

[Your Contact Information]