**RCA of CrowdStrike**

What exactly happened?

* 8 million Windows computers were impacted (1% of total machines)
* There was Blue Screen of Death (DSOD).
* Estimated damage is $5 billion.

Why did it happen?

App 3

App 2

App 1

Kernel Mode

User Mode

Drivers

* Applications interact with Kernel in Operating System (most secure mode), when they need resources.
* It makes requests to the OS, for the resources like drivers, and they are granted by OS.
* Benefit of having two modes – If an application goes sideways or crashes, it will crash is user mode and the kernel mode will still be safe and secure.
* Falcon application of CrowdStrike:
  + Anti malware software running on Kernel mode.
  + WHQL - > Windows Hardware Qualified Lab, Certified software to run in Kernel mode.
* The underlying components of Falcon periodically get updates.
* An update happened on July 19 – C – 00000291 – XXX, where files in Falcon software was updated and new component version was deployed on windows machines.
* This update had a bug, and it was running in Kernel mode, which caused the BSOD.

How is it being resolved?

* To reboot the computer into safe mode.
* In safe mode, find any file with -291 extension and delete that file, and go ahead and reboot.
* Why was it difficult to resolve?
  + A lot of servers don’t have a GUI connected to them.
  + If a system is using BitLocker, it becomes more difficult to drill down to safe mode.
* Microsoft updated their recovery tool on July 22nd
  + Boot from WinPE.
  + Recover from Safe mode.

More technical Drilldown of the actual cause and what exactly was the bug:

* In the Channel file 291, there was an instruction to access data element number 21, but the data structure only contained 20 items.
* This caused an out of bound exception.
* Ultimately causing the system crash, as it occurred at the Kernel level.

Can customers of CrowdStrike financially recover?

* They may have insurance themselves, or they may try to utilize insurance of CrowdStrike.
* They may try to sue CrowdStrike directly, which is what Delta Airlines is trying to do, as they had to cancel 6k flights, impacting 0.5 million people.
* Terms and conditions of customers, with CrowdStrike, and what are the liabilities.

What Companies need to do in future?

* Estimate the probability of such an outage to occur, and the impact that it can have.
* It is important for Companies to have a Plan B, for such an outage.
* If the Company opts to have a low-level malware protection, then the company needs to ensure that the business continuity and management needs to be done properly.
* Some of the major metrics need to be implemented, like testing results on a preprod environment.
* Companies need to have all the stakeholders together, to discuss about how to set up a proper incident management system.