Lessons from the Crowdstrike Falcon Outage:

The importance of business continuity planning for your organisation

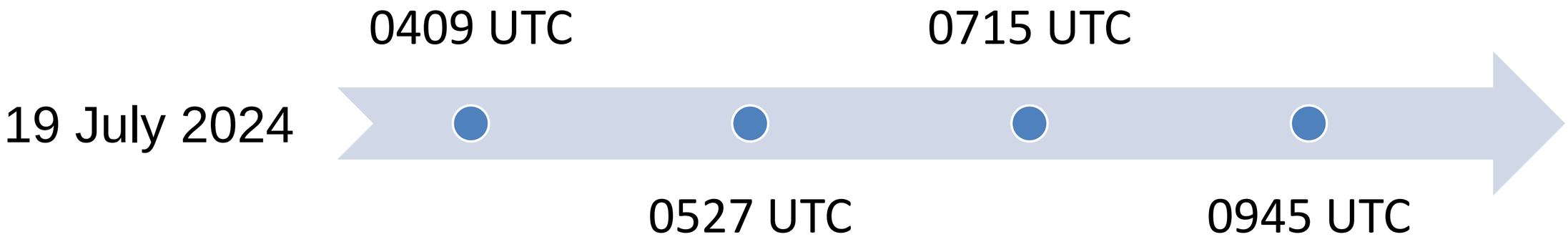
Dr John Selby
Principal Consultant | Head of Research, Privcore
Honorary Fellow, Macquarie University

Overview

1) What happened? -|
2) Why did it happen? -|→ Incident Analysis
3) What were the consequences? -|

4) What is BCP? -|
5) Why is BCP relevant? -|→ Risk Exposure Reduction
6) How does BCP differ from DRP? -|
7) How can improving your BCP increase your organisation’s resilience? -|

Crowdstrike Falcon Incident…



0409: Crowdstrike released to its Falcon users Channel File 291 as a security configuration update

- An extra array field (21 instead of the intended 20) was included
- Crowdstrike Falcon ran as a driver in Ring 0 on Windows PCs with elevated privileges, resulting in an invalid page fault
- Falcon users who applied the update on PCs running Microsoft Windows 10 & 11 experienced a blue screen of death
- Those PCs became stuck in a bootloop or recovery mode requiring an in-person fix

0527: Crowdstrike released a fixed version which meant that PCs that booted after that time were not affected

0715: Google blames Crowdstrike’s update for the fault

0945: Crowdstrike CEO revealed the problem was not a cyber attack and that a fix had been deployed

Crowdstrike Falcon Incident…

Root cause analysis of technical issues:

- Failure to adequately test updates prior to release
- Failure to validate the number of fields in the template type when compiling the sensor
- Failure to conduct a runtime array bounds check on Channel File 291
- Failure to check the Content validator for logic errors
- Failure to stagger release of updates so that technical problems could be detected/fixed sooner

Business Imperatives:

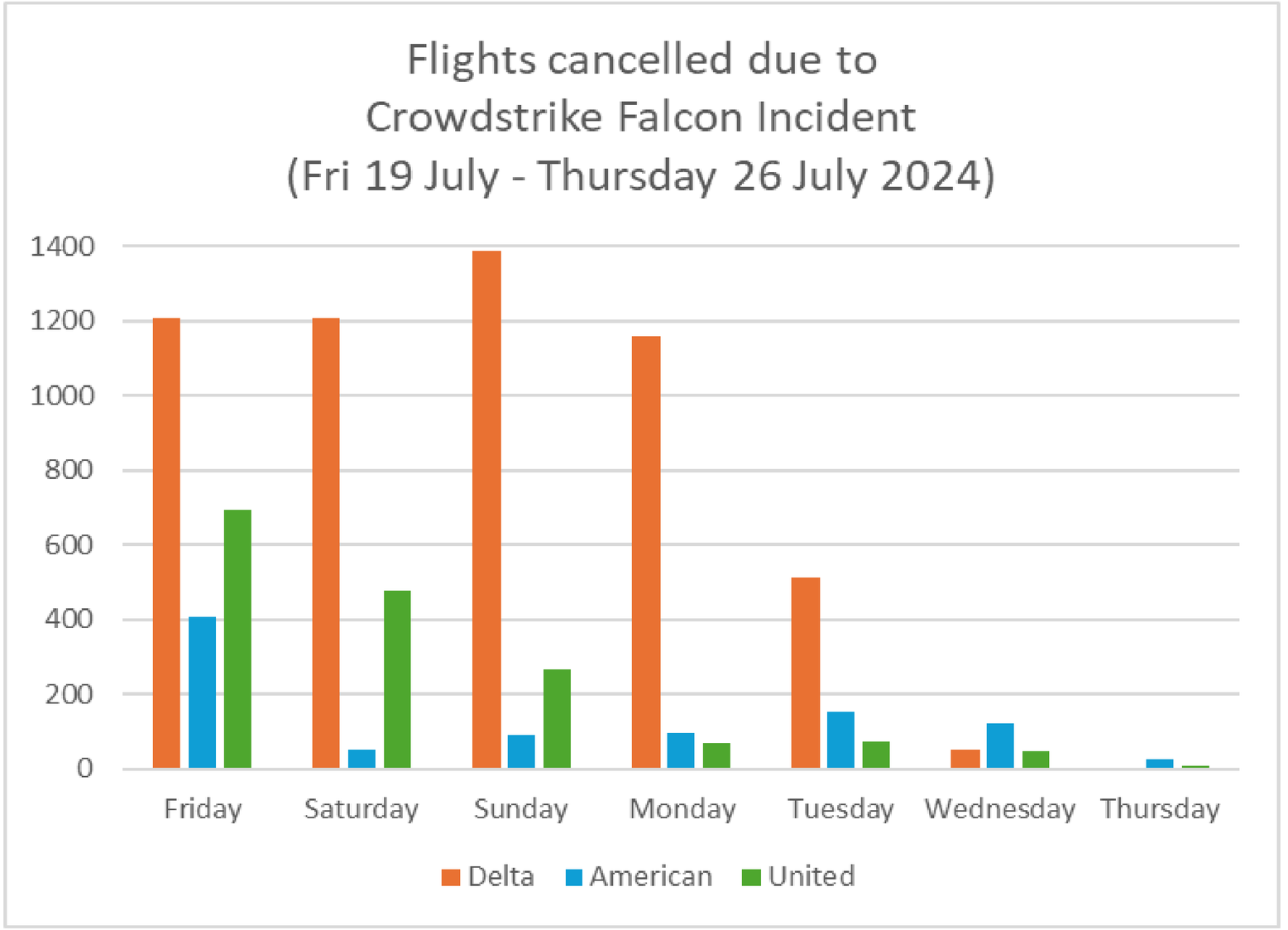
- Prioritising fast release of updates (cybersecurity product) over reliability of updates

… Rippled through its customer base

- 60% of Fortune 500 companies deployed Crowdstrike Falcon
- 34 000 flights delayed & 5 078 cancelled on the first day
  (~4.5% of all flights)
- Thousands of passengers sleeping on floor at Atlanta airport
- Surge pricing – train ticket prices soared
- Hospitals cancelled surgeries
- TV stations went offline
- Thousands of hotels unable to check in customers
- Bank systems hit + millions of workers unable to receive regular paychecks

Image source: GenAI

Recovery time varied between organisations



Why did some organisations recover faster than others?

Content removed from web version.

Contact operations[at]privcore.com for further information.

Lawsuits… so many lawsuits

Content removed from web version.

Contact operations[at]privcore.com for further information.

What is Business Continuity Planning?

Content removed from web version.

Contact operations[at]privcore.com for further information.

Why prepare a Business Continuity Plan?

Content removed from web version.

Contact operations[at]privcore.com for further information.

Questions?

Contact

Dr John Selby
Email: selby[at]privcore.com
Web: www.privcore.com