Case 6: CrowdStrike Outage

Module 6: What Powers the Financial System?

Background

Modern financial infrastructure runs on layered software. At the bottom are operating systems (primarily Windows and Linux), on top of which sit databases, communication protocols, trading engines, and risk management systems. Threaded through all of these layers is cybersecurity software – programmes that monitor systems for threats, block malicious activity, and report anomalies. As covered in M6L2 (Core Banking) and M6L4 (Next-Gen Infrastructure), the financial system depends on this software stack functioning continuously. A failure in any layer can cascade upward.

CrowdStrike Holdings is an American cybersecurity company founded in 2011. Its core product, Falcon, is an endpoint detection and response (EDR) platform. An "endpoint" is any device connected to a network – a laptop, a server, an ATM. Falcon runs at the kernel level of the operating system, meaning it has the deepest possible access to the machine's functions. This is necessary for security software to detect sophisticated threats, but it also means that a malfunction in Falcon can crash the entire system – not just the application, but the operating system itself.

By mid-2024, CrowdStrike's Falcon was installed on approximately 24 million endpoints worldwide. Its customers included banks, stock exchanges, airlines, hospitals, and government agencies. The company's market capitalisation exceeded USD 70 billion. Falcon had become part of the critical infrastructure that critical infrastructure depends on.

What Happened

On July 19, 2024, at approximately 04:09 UTC, CrowdStrike pushed a routine configuration update to Falcon sensors running on Microsoft Windows systems. The update was a "channel file" – a small data file that tells Falcon what threat patterns to look for. Channel file updates are pushed frequently (sometimes multiple times per day) and typically do not require a system restart.

This particular update – Channel File 291 – contained a logic error. When Falcon attempted to process the file, it triggered an out-of-bounds memory read in the Windows kernel. This caused the operating system to crash with a "Blue Screen of Death" (BSOD) and enter a reboot loop. Because Falcon loads at startup before most other software, the system would crash again on every restart. The machines were effectively bricked – unusable until a manual fix was applied.

Approximately 8.5 million Windows devices were affected worldwide. The impact was immediate and broad:

Banking and payments: Multiple banks reported that their ATM networks went offline. Point-of-sale terminals at retail locations failed. Internal banking systems used for transaction processing and risk management were disrupted. Some banks could not process wire transfers or clear trades for several hours.

Stock exchanges: Several exchanges experienced delays in opening. Trading firms reported that their order management systems crashed, preventing them from participating in early trading. Market data feeds were disrupted.

Airlines and logistics: This was the most visible impact. Major airlines grounded flights because their check-in and boarding systems ran on affected Windows machines. Airports displayed handwritten flight information. The cascading flight cancellations lasted for days.

Recovery: CrowdStrike identified the issue within approximately 79 minutes and reverted the channel file. However, machines already in a boot loop could not receive the fix remotely. Each affected device required manual intervention: booting into Safe Mode, navigating to the CrowdStrike directory, and deleting the faulty channel file. For organisations with thousands of devices across multiple locations, this process took days.

Parametrix, a cloud-monitoring firm, estimated that the outage caused approximately USD 5.4 billion in direct losses for Fortune 500 companies alone. CrowdStrike's stock price dropped approximately 11% in the following trading session.

The Analysis

The CrowdStrike outage is not a story about a cyberattack. No adversary was involved. It is a story about concentration risk in software supply chains – the same concept that M6 applies to payment rails and banking infrastructure, now applied to the tools that protect that infrastructure.

The financial system's dependence on a small number of critical software vendors creates a form of systemic risk that traditional risk models do not capture well. When a single update from a single company can simultaneously disable ATMs, trading systems, and payment processors across multiple countries, the software supply chain has become a single point of failure (M6L4, Next-Gen Infrastructure).

Several structural factors amplified the impact:

Kernel-level access. Security software operates at the deepest level of the operating system by design. This is not a flaw – it is required for the software to do its job. But it means that a bug in security software is more destructive than a bug in an ordinary application.

Automatic updates without staged rollout. The channel file was pushed to all customers simultaneously. A staged rollout – pushing the update to 1% of devices, monitoring for problems, then gradually expanding – would have limited the blast radius to thousands of machines rather than millions.

No pre-deployment testing of this specific file type. CrowdStrike's quality assurance processes did not catch the logic error in Channel File 291 before deployment. The company later disclosed that its content validation system had a gap for this particular type of configuration update.

Manual recovery required. Because the crash occurred at the kernel level before network connectivity was established, remote remediation was impossible. Every affected machine required physical or local access – a recovery model that does not scale.

The CrowdStrike incident prompted regulatory attention to software supply chain concentration. Financial regulators in the EU, UK, and US have since intensified their focus on third-party risk management and operational resilience requirements for financial institutions, building on frameworks like the EU's Digital Operational Resilience Act (DORA).

Discussion Questions

1. Using M6L2 (Core Banking) and M6L4 (Next-Gen Infrastructure), explain why the financial system's dependence on shared software vendors creates concentration risk that is different from traditional financial risk.
2. CrowdStrike pushed the faulty update to all customers simultaneously rather than using a staged rollout. Compare this to the deployment safeguards discussed in M5L4 (MLOps) and explain how staged deployment practices from software engineering could apply to security software updates.
3. The EU's Digital Operational Resilience Act (DORA) requires financial institutions to manage third-party technology risk. Evaluate whether DORA-style regulation could have reduced the impact of the CrowdStrike outage, drawing on M7L2 (RegTech).
4. If you were the CTO of a mid-sized European bank on July 18, 2024 (the day before the outage), what operational resilience measures could you have had in place to maintain basic banking services during a system-wide software failure?
5. Could the financial system reduce its dependence on a small number of cybersecurity vendors, or is concentration in security software an unavoidable feature of the current technology landscape?

Further Reading

- CrowdStrike (2024). *Preliminary Post Incident Review: Content Configuration Update Impacting the Falcon Sensor*. Published July 24, 2024.
- Parametrix (2024). *CrowdStrike/Microsoft IT Outage: Preliminary Insured Loss Estimates*. July 2024.
- European Union (2022). *Regulation (EU) 2022/2554: Digital Operational Resilience Act (DORA)*. Official Journal of the European Union.