Delta Air Lines passengers in Atlanta trying to find their bags on July 22 after flights were cancelled or delayed as a result of the CrowdStrike outage on July 19. The CrowdStrike incident highlights a fundamental paradox in cyber security: centralised solutions offer streamlined management but create a single point of failure. PHOTO: GETTY IMAGES VIA AFP

CrowdStrike crash: When protectors become the problem

Centralised cyber-security solutions add to efficiency but can also create a single point of failure.

Kelvin Law

On July 19, a routine software update from cyber-security giant CrowdStrike went catastrophically wrong. The update triggered a cascade of system failures that paralysed businesses and critical infrastructure worldwide. This wasn't a hack or a cyber attack. Instead, the culprit was a faulty code update – a routine maintenance gone wrong.

The timing couldn't have been worse. As Friday afternoon settled in across Asia, many companies were heading into their busiest periods before the weekend. By the time New York woke up, the problem had snowballed into a full-blown crisis.

The scale of the impact was staggering. From the United States to Europe, and across Asia, numerous businesses and critical infrastructures found themselves at a complete standstill: airlines had to ground flights, leaving travellers stranded. Hospitals grappled with system failures, potentially putting lives at risk. Even carparks weren't spared, with vehicles queueing up in front of unresponsive gantries.

WHAT IS CROWDSTRIKE?

To understand the magnitude of this incident, we first need to grasp what CrowdStrike does. CrowdStrike is a leader in cyber security. Imagine a team of elite digital bodyguards, constantly on the lookout for threats to your computer systems. That's essentially CrowdStrike's role in the cyber-security world. They're the ones who are supposed to keep the bad guys out of our digital homes.

CrowdStrike prides itself on safeguarding organisations from cyber threats. One of its marketing taglines, "62 minutes could bring your business down", was meant to showcase the importance of robust cyber security. In a twist of bitter irony, its own update proved this point all too well, bringing countless businesses and infrastructures to a screeching halt for far longer than 62 minutes.

While this incident involved CrowdStrike, it's important to understand that this is a symptom of a larger issue: the deep integration of third-party software in our digital infrastructure and the risks this brings.

Think of it like a house of cards – removing one card can cause the entire structure to collapse. This vulnerability could affect any company's software, regardless of its size or market position, highlighting weaknesses in our digital infrastructure rather than problems unique to one company.

THE ROOT OF THE PROBLEM

To understand this incident, we need to look back to 2009. That year, Microsoft reached an agreement with the European Commission, allowing third-party security companies to integrate their products more deeply with Windows. While this decision fostered a more competitive software environment, it also created new risks.

It's like allowing multiple locksmiths to have master keys to your house – it provides more options for security, but also increases the potential points of failure. This agreement paved the way for companies like CrowdStrike to offer robust protection, but as we've seen, it also meant that issues with their software could have system-wide impacts.

It's vital to understand that CrowdStrike's updates operate independently of Windows updates, meaning they can occur even if you haven't pressed the Windows "update" button. This level of access is necessary for real-time threat protection. However, it also means that any issues with these unstoppable security updates can have far-reaching consequences.

This interconnectedness is both our strength and our pain point. The same systems that allow for unprecedented efficiency and global collaboration also create vulnerabilities. Balancing protection and exposure is a delicate act. Ironically, each new security measure might introduce unforeseen vulnerabilities.

A Reddit user summed up the technical challenge bluntly: "This will require booting millions of machines into recovery and removing files."

This wasn't a problem that could be solved with a simple reboot or a quick patch. Each affected system needed individual attention, a process that could take days or even weeks for large organisations and critical infrastructure.

It's akin to having to manually restart and unlock every traffic light in a city after a power outage, but imagine some encrypted traffic lights require a unique 48-character password. This herculean task would be daunting even for the most skilled IT professionals, let alone for organisations dealing with thousands of affected systems. The cost in terms of lost productivity and potential data loss is still being calculated, but it could run into billions of dollars globally.

THE CENTRALISATION PARADOX

The CrowdStrike incident highlights a fundamental paradox in cyber security: Centralised solutions offer streamlined management but create a single point of failure. While spreading out the system might seem like a solution, it comes with its own challenges. A balanced approach could be the way forward, using centralised functions for core security operations while having backup systems ready as a safety net.

Organisations should explore ways to create backup systems and partially separate critical functions. This means having backup systems ready to take over if the main system fails, like having a backup generator for a hospital. Keeping some essential operations isolated from the main network can help prevent a single problem from bringing down an entire organisation. A cautious update strategy, like testing updates on a small group of computers first with an automatic undo feature, could significantly reduce the risk of widespread outages due to faulty updates.

We also must recognise that cyber threats don't adhere to a 9-to-5 schedule. Our contingency plans need to be operational round the clock, including weekends and holidays. It's like having a fire department that never sleeps – because in the digital world, a "fire" can start at any moment. Just as buildings conduct regular fire drills, organisations should periodically test their cyber incident response plans. These "digital fire drills" ensure that when a real crisis strikes, everyone knows their role and can act swiftly, regardless of the hour.

In the event of an incident, swift communication and rapid updates to affected businesses or organisations should be a top priority, even if they are outside of normal business hours. In our interconnected digital economy, every minute of downtime can translate to significant financial losses and lasting reputational damage.

In the digital age, our security is only as strong as our weakest link – and as the CrowdStrike incident shows, even our strongest defenders can sometimes become that link.

• Kelvin Law is associate professor of accounting at Nanyang Technological University's Nanyang Business School.