CrowdStrike outage

The CrowdStrike outage **explained for business owners and managers**

yourIT/man

On Friday 19th July 2024, a routine software update from CrowdStrike, a leading cyber security company, caused a major issue affecting an estimated 8.5 million Windows computers.

This incident led to significant disruptions in many sectors, including airports, supermarkets, and media.

Here we explain what CrowdStrike is, what went wrong with the update, how it impacted businesses, and how to protect **your business**.

What is CrowdStrike?

CrowdStrike is a leading cyber security company, founded in 2011 and based in the United States. Essentially, they act as digital bodyguards for businesses and large organisations, protecting them from cyber threats like ransomware, malware, and other online attacks.

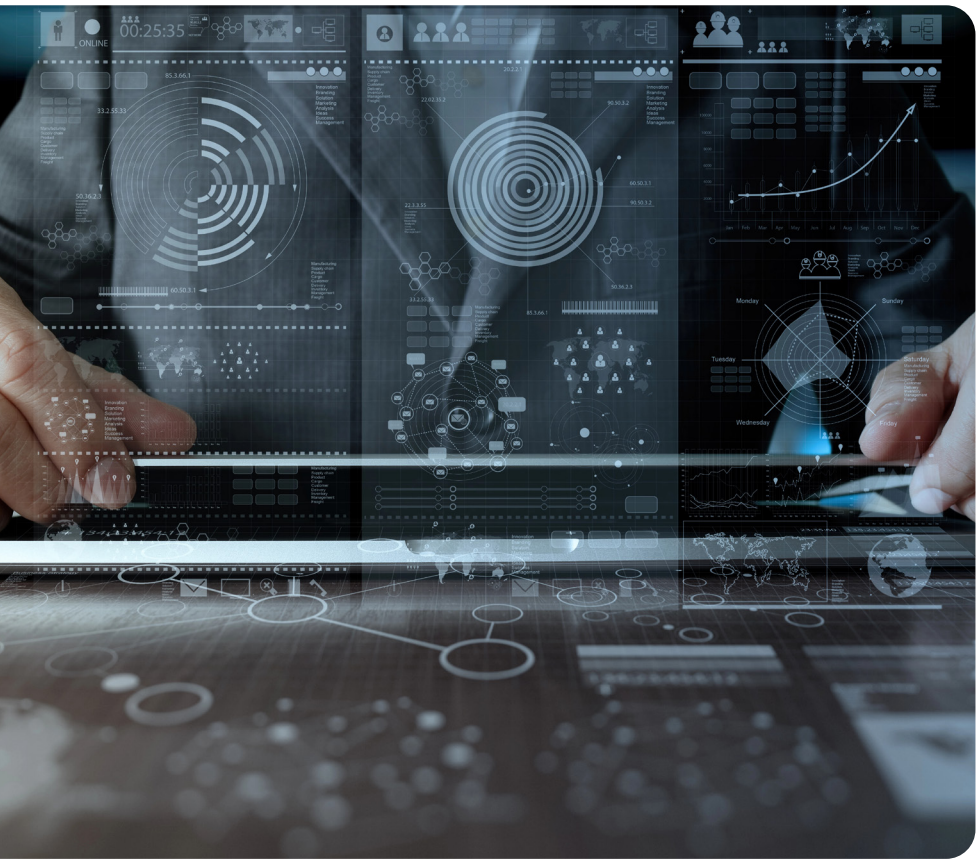
CrowdStrike is trusted by a wide range of businesses, including more than 500 companies from the Fortune 1000 list. They have a solid reputation for responding quickly to cyber threats and have been involved in investigating major cyber incidents.

Their main product is called the Falcon sensor program. This cloud-based security system is designed to detect and stop cyber threats in real time.

What is Falcon sensor?

Think of your computer as a house. Regular antivirus software is like a security system that looks for specific types of bad guys (like burglars) that it recognises from before. If it sees any of these known bad guys, it stops them from getting in.

Falcon sensor is something more, called an EDR (Endpoint Detection and Response). It's like having a smart security guard for your house. This guard not only looks for the bad guys that the antivirus knows but also keeps an eye out for any strange or suspicious activity. The guard can also investigate unfamiliar situations and take action to protect your house, even if the threat is something new.



So, while an antivirus is good at stopping known threats, an EDR is much better at handling new and unexpected threats to keep your computer safe. The trade-off is that EDR requires a deeper level of access.

EDR requires rapid updates to stay on top of quickly changing threats. Unlike other software updates, these can't be rolled out in stages.

What happened?

On 19th July, a routine software update from CrowdStrike caused major disruption for many businesses around the world.

Early that morning, CrowdStrike released an update to their Falcon sensor program. This update was intended to improve security by targeting specific tools used in cyber attacks. But the update contained a coding mistake, known as a "logic error."

This mistake caused Windows computers running Falcon sensor to crash, leading to the infamous "Blue Screen of Death" (BSOD).

The impact was immediate and widespread.

Many businesses found their Windows computers unusable, resulting in significant disruption. Airports experienced chaos as their systems failed, supermarket checkouts malfunctioned, and journalists faced difficulties reporting on the issue due to their equipment crashing.

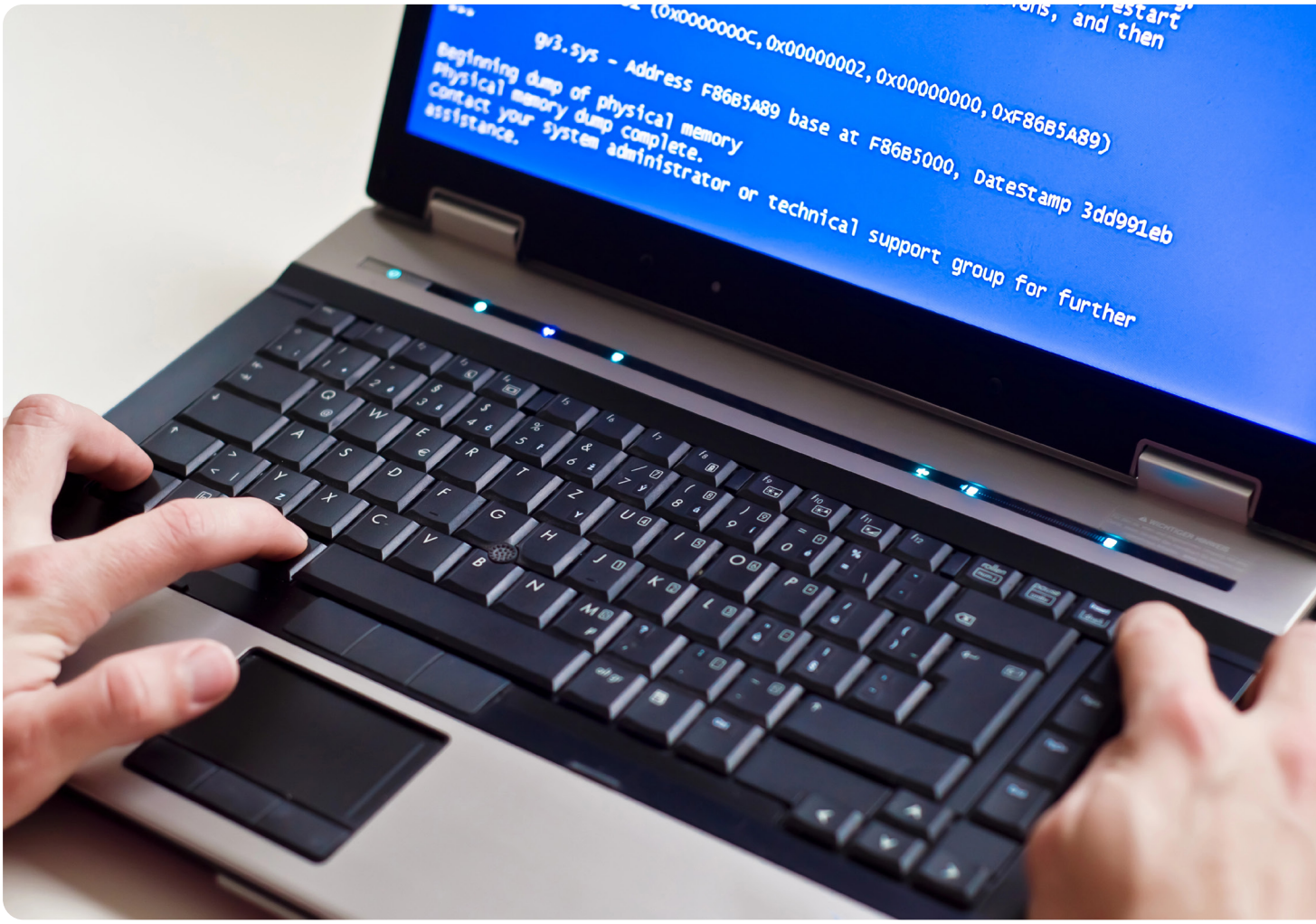
The problem affected millions of devices globally. People reported that their computers went into a reboot loop, making it impossible to use them.

CrowdStrike responded quickly. Within an hour of identifying the issue, they began working on a fix. By 5:27am UTC, they released an update to correct the faulty configuration files.

But the recovery process varied. For many, the issue could be resolved remotely by deleting the problematic file if the system was online. For those with offline systems, manual deletion of the file was necessary, which often required help from IT support.

What was the impact on businesses

The CrowdStrike outage had a huge impact on businesses across many sectors.



Airports and airlines

The outage led to significant disruptions at airports. Systems that manage flight schedules, ticketing, and customer service were hit, causing delays and confusion. Passengers experienced long lines and delays as airport staff struggled to manage without their usual digital tools.

Supermarkets and retail

Many supermarket checkouts malfunctioned, making it impossible to process sales. This led to frustrated customers and lost sales as stores struggled to operate without their point-of-sale systems. Some retailers had to close temporarily until their systems were restored.

Media and journalism

Journalists and media companies faced major challenges as their computers crashed, leaving them without the essential tools needed to report on the incident. This disrupted news coverage and the ability to provide timely updates to the public.

Banks and financial services

The financial sector also felt the impact, with banks experiencing system outages that affected transactions and customer service. Online banking services were disrupted, leading to difficulties for customers trying to access their accounts or perform financial transactions.

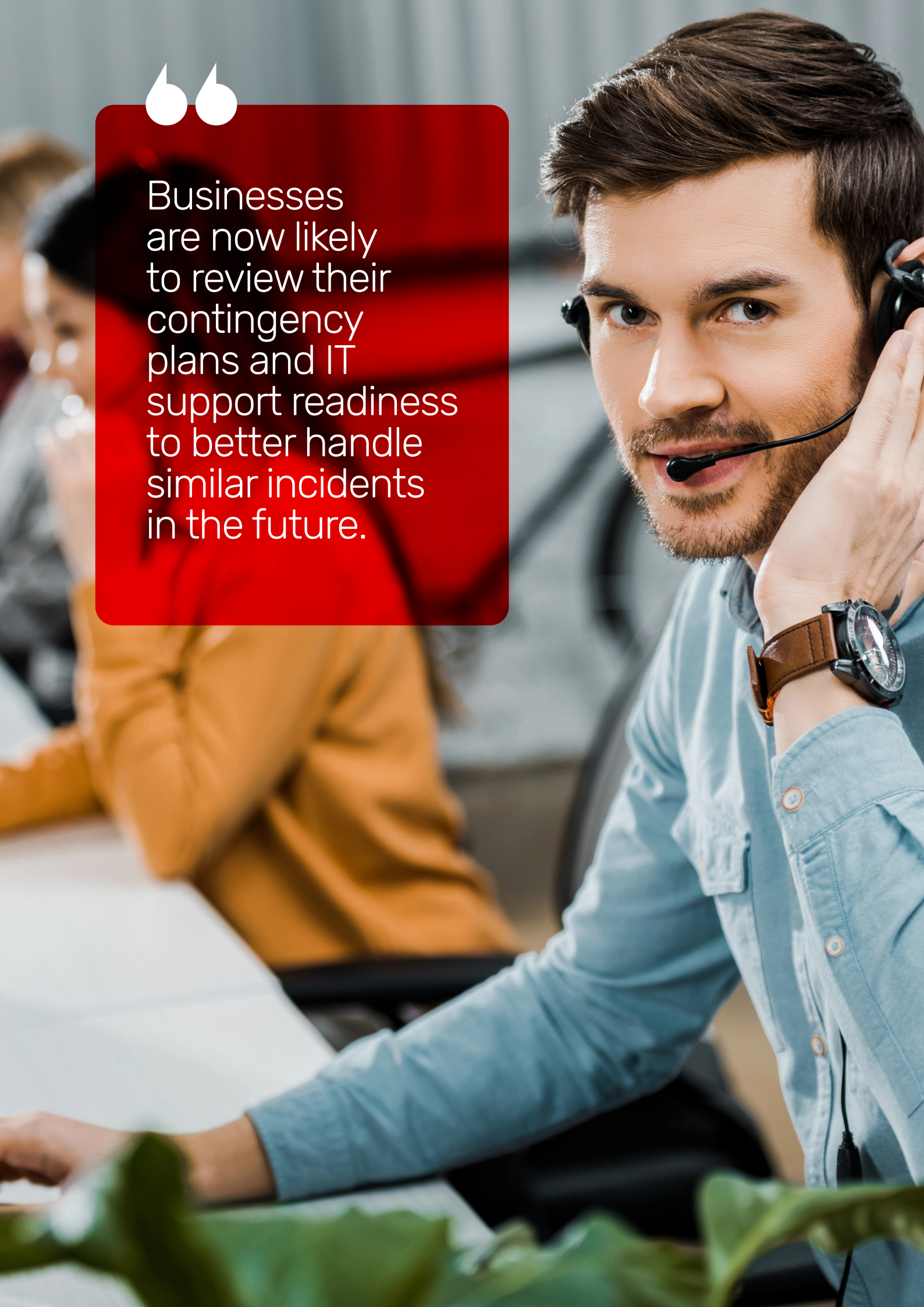
General business operations

Across the board, businesses that relied on Windows systems experienced productivity losses. Employees were unable to access important files, communicate effectively, or perform their usual tasks. Many companies found it difficult to provide customer support as their systems were down. Call centres and online help desks faced increased volumes of queries and complaints, further straining resources.

Healthcare

While not as widely reported, healthcare institutions using affected systems could have faced delays in accessing patient records, scheduling, and other critical operations, potentially impacting patient care.

Overall, the CrowdStrike outage demonstrated how critical reliable cyber security tools are for business continuity. It highlighted how interconnected modern business operations are and the widespread impact that a single software issue can have.


Businesses are now likely to review their contingency plans and IT support readiness to better handle similar incidents in the future.

Can this happen to us?
Why SentinelOne is different

SentinelOne's security updates are confined to detection-related knowledge and security models. These operate in an isolated user-mode space, separate from the core security agent. These updates do not affect the Operating System or core components of the SentinelOne agent. Since their agent primarily operates in user-space, security updates only impact user-environment components. This is an intentional design choice by SentinelOne to increase stability and significantly decrease interoperability risks.

Core components of SentinelOne agents are updated through an upgrade policy process, which Your IT Man manage for their customers. Despite SentinelOne offering us early access builds of their software, we only rollout General Availability updates to our customers. This maximises compatibility and provides a stable and well-tested system before any deployment. All security update rollouts are closely monitored by SentinelOne and have a phased rollout across all customers.procedures to help mitigate the impact of future disruptions.

At Your IT Man we pursue best-of-breed managed services in all areas of our productivity and security stack. We're proud of the products we offer our customers. We ensure that at all times the products we offer suit your needs and provide maximum ROI.
This is why we protect using SentinelOne.

How we can help your business

Many businesses are now reviewing their disaster recovery plans and business continuity software. They want to be sure they have clear procedures to help mitigate the impact of future disruptions.

Ask us to review your current operations or plan a strategy to make sure your business is protected.

Get in touch.

CALL: 0333 023 3100
EMAIL: contactus@youritman.com
WEBSITE: youritman.com

yourIT/man