Microsoft & CrowdStrike Outage

Microsoft & CrowdStrike outage **explained**

✓ **Business Leaders**
✓ **IT Managers**

Why Microsoft Azure & Office 365 is not invincible. The Global Impact you saw on the news

breathetechnology
support | cloud | security | infrastructure | comms
EMPOWERING YOU THROUGH SECURE TECHNOLOGY

www.breathetechnology.com

A word from our MD

The great Office 365 Myth: **Office 365 is Unbreakable and Safe**

Craig Van Aswegen
MD & Snr IT
Management Consultant
Breathe Technology LTD

> “The disruption was caused by a defective update from the cybersecurity firm CrowdStrike, which impacted Microsoft Windows systems globally.”

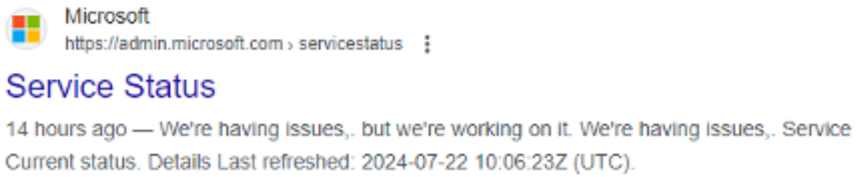
Often, when it comes to IT, there are misconceptions about how things work and specifically where systems have risks around reliability, performance, or cyber security. Until it breaks and it causes disruption, inconvenience, or even financial loss. Then we’re quick to react to the problem and to find ways to fix it and avoid it from happening again. Obviously, the better approach would have been to set it up with the correct measures from day one. Lack of understanding and avoidance of IT spend are often the main reasons we see.

Microsoft experienced a significant global outage on July 19, 2024.

The disruption was caused by a defective update from the cybersecurity firm CrowdStrike, which impacted Microsoft Windows systems globally. This led to widespread issues, including over 8.5 million devices being affected, causing Blue Screen of Death (BSOD) errors and making systems unresponsive.

Other software vendors that provide cloud services also experienced issues as they hosted their systems in Microsoft Azure.

The outage had extensive repercussions across various industries. It disrupted flight operations, resulting in thousands of flight cancellations and delays worldwide. Airports, including those in the US and UK, were heavily impacted, with some services experiencing prolonged issues even after the initial disruption. Additionally, many businesses, hospitals, and other critical services experienced operational difficulties due to the outage. Including various customers that Breathe support.



Microsoft
https://admin.microsoft.com › servicestatus

Service Status

14 hours ago — We're having issues,. but we're working on it. We're having issues,. Service Current status. Details Last refreshed: 2024-07-22 10:06:23Z (UTC).

What's the moral of the story?

Office 365 is great. The fact that it's cloud hosted by Microsoft provides a clear level of resilience that most businesses couldn't do if the still hosted their own servers. However, it's clearly not invincible and the fact that it's open the whole world poses some significant security risks.

Our advice

Use the same principle to protect your data and system as you would have when you owned the systems and hosted them inhouse.

Examples include:

1. Deploy username and password protection. It's open to the outside world, you need to enable two factor or multi factor authentication to secure your username and password

2. Scan your data for malware and viruses. Yes, it has Microsoft Defender built in. But most people don't actually check the Defender functionality that's included with your standard licensing. Either license it correctly and use the fully featured version of Defender or use an expert vendors software like SonicWall CAS (Cloud Application Security) to scan your data in SharePoint, OneDrive, MS Teams, Exchange Email Online etc. It acts in a very similar way to Anti-Virus did on your server.

3. **Deploy Account Take over protection.**
   Account-takeover attacks against Microsoft 365 users are spiking, driven primarily by a surge in credential theft and successful phishing attempts. In 2021, roughly 20% of organisations that use Microsoft 365 suffered at least one account compromise.

   Once cybercriminals have taken control of one of your Microsoft 365 accounts, they are able to explore and steal your cloud-hosted data, move laterally to compromise further accounts, use impersonation to execute financial fraud, infiltrate ransomware or other malware, and potentially cripple your ability to operate. They can also use compromised accounts to launch highly effective attacks against your customers, employees, and business partners.

   Needless to say, these are things that it's worth some effort and investment to prevent.

   Breathe use SonicWall CAS for this protection. The same software used to scan Office 365 for Malware.

4. Scan your email for Spam. In our view Microsoft Defender is not enough. Defender is your last stand. Like Anti-Virus on your server. The better scenario is to scan emails and clear spam, emails

with malware or phishing attacks before the land in your Office 365 email server. Breathe use an application call ProofPoint.

Proofpoint Email Protection is the industry-leading email gateway, which can be deployed as a cloud service or on premises. It detects both known and unknown threats that others miss. Powered by NexusAI, the advanced machine learning technology, Email Protection accurately classifies various types of email.

5. Enable GEOIP. A simple setting in Office 365 that could eliminate 80% of attacks. GEOIP works by blocking access from entire countries. Unfortunately, the reality is that most hacking attempt originate from specific countries. It doesn't help that Europe is at work. Ask yourself the question, what is the benefit in leaving the account open to access from other countries? If there are specific countries that need access, allow them only.

6. Enable conditional access. Office 365 Conditional Access is a security feature that helps you protect your data by controlling how and where users can access Office 365 services. Think of it as a set of rules or policies that control this access. An example may be that it has to be from a company laptop or PC and be within the UK.

7. Setup DMARC. It is a bit like what SSL or HTTPS is for websites. It secures your email domain and protects unauthorised access such as spoofing. When someone impersonates you are your staff.

8. Ensure you have a working and tested backup. So, everyone says they have backup… but do you really. It's important to understand exactly what has been backed up and how often. This should not be an IT decision. It's a wider management decision. It simply implements and manages the system. Backups should also be tested and the management team needs reporting to confirm this is in place and working.

If you have questions, comments or need help, please let Lucy@breathetechnology.com know or call us on:

London	020 3519 0124	**Suffolk**	0144 059 2163
Cambridge	0122 320 9920	**Sheffield**	0114 349 8054

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 the 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 programme. 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 programme. 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 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.

However, 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 of the outage?

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

```
                                ,0x00000002,0x00000000,0xF86B5A89)
 3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

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.

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

How we can help you?

Many organisations are now reviewing their cyber security and disaster recovery plans, as well as their business continuity setups.

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 school is protected.

Get in touch.

www.breathetechnology.com
(live chat available)

London	020 3519 0124
Cambridge	0122 320 9920
Suffolk	0144 059 2163
Sheffield	0114 349 8054

lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms