Does the flap of a butterfly's wings in Brazil set off a tornado in Texas? The impact of the CrowdStrike outage on supply chain risk

Patrick Hill
Partner
T: +44 (0) 20 7894 6930
phill@dacbeachcroft.com

Camilla Elliot
Solicitor
T: +44 (0) 20 7894 6363
celliot@dacbeachcroft.com

The outage of global cyber security firm CrowdStrike's systems on 19 July 2024 sent ripples through industries worldwide. Airlines were unable to check in passengers, hospitals left unable to carry out appointments and banks unable to pay customers. The UK National Cyber Security Centre was forced to issue an urgent warning that opportunistic malicious actors were seeking to take advantage of the outage.

Microsoft estimated that 8.5m computers worldwide were affected by the corrupted software update, amounting to approximately 1% of the world's Windows machines, yet the impact was felt much more widely. As David Weston, vice-president of Microsoft, observed: *"the broad economic and societal impacts reflect the use of CrowdStrike by enterprises that run many critical services".*

Almost half of all Fortune 500 companies utilise CrowdStrike's cyber security systems, meaning that this failure dramatically illustrated the systemic fragility of globally inter-connected digital infrastructure. The figures from Microsoft imply that the CrowdStrike incident was the largest cyber event in history. By way of comparison, the WannaCry attack in 2017, widely recognised as one of the most destructive cyber-attacks and the closest event in scale to the CrowdStrike incident, is estimated to have impacted 300,000 computers in 150 countries.

The CrowdStrike incident triggered a number of questions for both the companies affected, with the widespread operational disruption serving as a wake-up call for supply chain risk management, catapulting it to the top of risk managers' agendas.

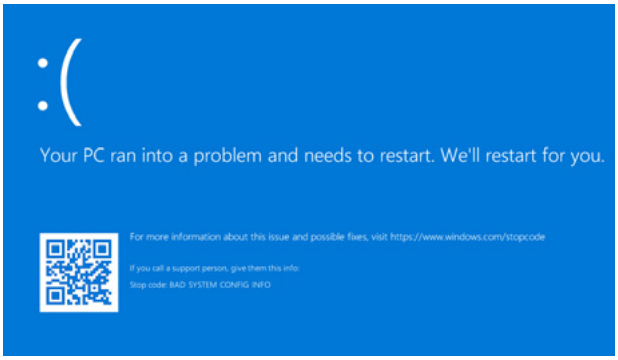
The incident also prompted discussions around the impact of recently introduced and forthcoming regulations on their cybersecurity measures, and the effect of contractual agreements in place. Cyber insurance companies were also left considering a number of possible coverage and liability issues.

Kelly Richards, Specialist Risks team leader and solicitor at Zurich Insurance comments:

> *"The CrowdStrike incident spread globally, following the sun. It shone a stark light on the challenges faced by the society, including the insurance industry, arising out of systemic events triggered without any 'bad actor' intervention."*

What happened?

In the early hours of 19 July 2024, CrowdStrike issued a defective update to Falcon, a piece of 'endpoint detection and response' (EDR) software. Falcon monitors systems on which it is installed, identifying threats and responding to them. Many software updates for these types of systems are set to download automatically and are, therefore, particularly risk prone. In this instance, the Falcon software update triggered a malfunction which caused affected units to show the Windows 'blue screen of death', as shown below:



Somewhat prophetically, George Kurtz, CrowdStrike's CEO and co-founder, had noted in a 2024 CrowdStrike report:

> *"the growing menace of supply chain attacks and exploitation of trusted software"*.

However, it is worth reiterating that this particular incident did not result from a supply chain attack or exploitation, it was a defective software update at fault. This highlighted the potential disruption which might be caused by other forms of software supply chain disruption, including interference with third-party code (whether malicious or otherwise), open-source applications and managed service provider (MSP) systems.

The net effect in terms of disruption to the global supply chain is identical whether the issue was caused by a software update (as in the CrowdStrike incident) or a malicious attack. The regulator of the UK financial service industry, the Financial Conduct Authority (FCA) stated this incident was the latest in a trend of third-party related incidents. Across 2022 and 2023, the FCA noted that:

> *"third-party related issues were the leading cause of operational incidents reported."*

Why was the incident so far-reaching?

A key contributor to the scale of the disruption was CrowdStrike's dominant market position in next-generation anti-virus/EDR solutions. The incident paralysed operations in aviation, healthcare networks, financial systems, global shipping and Government agencies during the 16-hour outage. It is estimated that CrowdStrike's virus monitoring agents were installed on over 500 million endpoints worldwide, with the defective software update causing many systems running Windows to crash during the rollout.

The dominance of a small number of vendors in the cyber security sector is an increasing trend. BCS, the Chartered Institute for IT commented that the incident reflected that:

> *"the world's digital systems have become more interconnected and interdependent."*

Greater reliance on a smaller number of players increases the potential for widespread disruption, meaning the scale of the disruption seen in this instance was magnified. The FCA stated *"these outages emphasise firms' increasing dependence on unregulated third parties to deliver important business services."*

Looking at specific examples of how the outage impacted certain sectors, healthcare systems for example, typically integrate large numbers of medical devices and patient health records. This can increase the number of third-party vendors with whom they are connected. In the UK, the outage meant that GPs were unable to use the NHS' systems for appointment booking, patient record management and sending prescriptions, with even high-priority tasks such as cancer referral letters being delayed. The Royal Surrey NHS Foundation Trust declared a 'Critical Incident' as radiotherapy appointments were forced to be rescheduled. The BMA described the day of the outage as *"one of the toughest single days in recent times for GPs across England."*

The aviation sector was also hit with the incident causing delays and operational challenges across the industry globally. As the outage hit airlines' reservation and scheduling systems, thousands of flights were cancelled worldwide. Across the 72-hour period of the outage, around 17,000 flights were cancelled – roughly 4% of all global flights – with Delta Airlines in the United States alone responsible for around 7,000 of these. Fortunately, safety was never compromised, as flights already in the air appeared to be unaffected.

Bank and card payment systems were affected by the outage, with some retailers temporarily resorting to cash-only transactions. Bankers at JPMorgan Chase had issues accessing company IT systems and RNS, the London Stock Exchange's regulatory news feed, was disrupted (although it was restored by early afternoon on the 19th). Markets themselves were affected, with the FTSE 100 closing down 0.6% (~£21 billion), and the United States' S&P 500 down 0.8% (~$336 billion).

As the dust settled on the incident, attention turned to the financial impact of the outage and who would bear any monetary burden.

Who picks up the tab?

To its credit, CrowdStrike has been commendably transparent in accepting full responsibility for the outage. Its President Michael Sentonas appeared in person to accept the 'Pwnie Award' for 'Most Epic Fail' in Las Vegas, and faced the embarrassment head on:

> *"Definitely not the award to be proud of receiving. I think the team was surprised when I said straight away that I'd come and get it because we got this horribly wrong. We've said that a number of different times and it's super important to own it when you do things well. It's super important to own it when you do things horribly wrong, which we did in this case.*
>
> *"The reason why I wanted the trophy is: I'm heading back to headquarters. I'm going to take the trophy with me. It's going to sit pride of place because I want every CrowdStriker who comes to work to see it because our goal is to protect people and we got this wrong, and I want to make sure that everybody understands these things can't happen and that's what this community is about.*
>
> *"So, from that perspective, I will say thank you, and I will take the trophy, and we'll put it in the right place, and make sure everybody sees it. So, thank you."*

4%
Of all global flights

17,000
Flights cancelled

72
Hour outage

And so, liability would appear not to be a major issue in terms of those companies affected. Or is it? It has been widely reported that CrowdStrike has insisted on limitation of liability clauses in its contracts. These are provisions in contracts that cap the amount of damages that one party can recover from another. In technology contracts, service providers like CrowdStrike prefer to include a favourable limitations of liability clause because it limits risk, generally by capping financial exposure in the event of a breach or other issue. Typically, limitation of liability clauses often excludes specific types of damages, such as consequential damages, and establish a cap on liability. This cap is typically defined using a fixed amount, a formula, or other financial metrics like 'fees paid' or 'fees paid or payable.' These will always be significantly less than the losses suffered.

CrowdStrike's standard terms and conditions limit its liability for contractual breaches to the fees paid by customers for its services. Experts say that unless a US court finds the clause is inherently unfair and unenforceable, CrowdStrike's customers will be unable to recover losses which exceed the fees paid under the agreement, or unless gross negligence can be established. Therefore, the position can be significantly altered by the contract between the parties, which can limit liability and even contain exclusion clauses which may be triggered.

Being unable to pursue CrowdStrike for financial losses, affected companies instinctively looked to their cyber insurance coverage. It is important to note that cyber policies do not just cover policyholders if they suffer a malicious attack (e.g. ransomware). Policies can provide cover if systems are taken offline due to a user error or similar, and therefore, the implications of the CrowdStrike event should be assessed by all insurance companies and businesses even if they were not affected in this instance. Importantly, there is very little standardisation of policy wordings in the cyber market. Generalisations are usually unhelpful. Some of the covers referred to below are standard clauses in policies, others are optional extensions for a prospective insured. Kelly Richards of Zurich Insurance adds:

> *"The cyber market is ever evolving and, often, provides some of the broadest covers available. Working with our broker and insured customers to provide support and ensure the extent of cover is understood, ideally before the occurrence of an incident, is key to what we do."*

System Failure

When assessing cover, the key factual enquiry is whether the policyholder used CrowdStrike Falcon, causing its own systems to be affected by the attack.

If so, there may be cover for System Failure – i.e., an unintentional malfunction or outage of the policyholder's IT systems. System Failure cover may be an extension to Business Interruption (BI) cover which is standard in most cyber policies and provides cover under the terms of the BI insuring clause. Whether the policyholder is entitled to cover under the other i.e. not BI Insuring Clauses in its policy following a System Failure, including incident response costs (to assist with deploying the fix to all of the affected devices) or liability (to respond to complaints/claims from customers affected by the CrowdStrike incident) will depend on the wording. Some wordings, however, may only provide cover for BI losses following a System Failure because the other Insuring Clauses are triggered by a malicious incident.

Supply Chain BI Losses

If a policyholder's systems were not affected directly (the policyholder did not have CrowdStrike Falcon installed), but it suffered some interruption to its business because its customers, clients, banks and/or members of its supply chain were impacted, there may still be cover under certain cyber wordings. Referring again to the lack of standardisation, there are broadly three potential avenues to cover for BI losses. The terms of the policies, particularly the definitions, will vary.

1. **Cover for losses caused by incidents affecting 'Providers' or similar:** this can be defined to include just IT services providers, such that if a policyholder uses CrowdStrike Falcon it may be entitled to cover even if they do not System Failure cover. Care should be taken, however, as some definitions focus on cloud computing providers (and the unavailability of information stored on the cloud), rather than IT providers, or even service providers, more generally.

2. **'Critical Supplier Cover' or similar:** this could be an additional cover or provided via an Endorsement. These can require the supplier(s) to be named in the Policy Schedule for cover to be extended.

3. **'Dependent Business Interruption Loss', or similar:** the availability of this cover should also be considered carefully. Again, it can be aimed at specific types of suppliers (e.g., cloud storage) and may not have cover as wide as a policyholder expects.

To reiterate, care should also be taken to identify exactly what the policyholder is entitled to if the BI Insuring Clause is triggered (for instance, whether incident response costs, liability etc., are included).

Can regulation help to limit the impact of future incidents?

Risk managers will be assessing their potential exposure to incidents affecting their supply chains, and the interplay of these exposures and regulatory obligations. The issues exposed by the CrowdStrike outage had arguably been anticipated by European legislators via two key pieces of legislation aiming to strengthen digital resilience.

From 17 January 2025, Regulation (EU) 2022/2554 covering digital operational resilience for the financial sector (DORA) has applied. DORA is a first piece of European-level legislation aiming to introduce a harmonised and comprehensive digital operational resilience framework for European financial institutions. In light of post-2008 financial services regulatory reform (which mainly focused on strengthening the financial resilience of the sector and, as such, addressed the information and communication technologies (ICT) risks as only a side matter), the European Commission's underlying intention for DORA is to address gaps in the European sectoral financial services legislation which, to date, has provided for a fragmented approach to operational resilience.

DORA also closely interacts with the Network and Information Security Directive (NIS2), an EU-wide piece of legislation both obliging Member States to adopt cybersecurity strategies, establish competent authorities and set out supervisory and enforcement obligations. Member States were required to implemented NIS2 into national law by 17 October 2024, although a number of Member States have not met that deadline.

Importantly, NIS2 imposes specific obligations regarding supply chains and obliges entities to consider vulnerabilities associated with each service provider and supplier. Sectors identified as 'high criticality' (such as energy, transport, banking, healthcare and digital infrastructure) as well as other critical sectors such as computing and digital providers (online search engines etc) are directly impacted by NIS2, with the Directive specifically setting out their necessary risk management measures and reporting obligations for specific entities. The legislation specifically recommends the integration of cyber security risk management measures into agreements with suppliers and service providers.

From a UK perspective, while NIS2 does not directly apply to UK businesses, the changes which came into force in January 2023 include adding managed service providers to the scope. As such, the NIS2 Directive applies to organisations operating or carrying out activities for EU businesses (including those in Ireland) within the scope.

Looking to the regulatory position in the UK directly, the existing Network and Information Security Regulations have long been identified by successive governments as requiring urgent update to reflect the need to keep pace with growing threats. A Cyber Security and Resilience Bill was announced in the King's Speech in mid-2024, which when introduced in 2025, will make *"crucial updates to the legacy regulatory framework"*. A number of changes expanding the remit of the NIS Regulation will be made, including the protection of more digital services and supply chains, specifically with reference to critical public services, akin to the NIS2. Regulators will be placed on a strong footing to ensure cyber security mechanisms are enforced and increased incident reporting will be mandated to provide better data on cyber-attacks.

What can we learn?

The global CrowdStrike IT outage demonstrated that even non-malicious cyber incidents may have serious repercussions. Events like these serve as a wake-up call for businesses to review their cyber resilience and to be prepared for more significant incidents in the future.

The FCA, offering general observations on the outage, noted that firms with clearly defined and tested communication strategies were able to quickly and efficiently issues responses and communicate with customers and other stakeholders.

Key takeaways from the CrowdStrike outage for businesses:

- Prepare for the worst. The widespread disruption caused by the outage illustrates the lack of effective backup systems in certain industry sectors necessary to ensure continuity. The FCA noted that those firms who had tested 'severe to but plausible' scenarios benefitted from this experience. The incident revealed that certain sectors (notably aviation and health) appeared to have insufficient contingency plans in place to cover a failure by a third-party software vendor.
- This incident was not malicious, but offers warnings about what might happen if a malicious attack were to be made on a similar scale.
- Understand your legal rights and obligations. Check contracts with suppliers to understand your potential exposure should the worst happen.
- Reliance on a single supplier. Beware of over-dependency on a single or small number of suppliers, and potential vulnerabilities as an industry sector. The incident may result in organisations diversifying their critical system supply chains.
- Understand the extent of your insurance coverage.

Full list of references available upon request