LOCKTON

Cyber

PROTECTING YOUR BUSINESS FROM IT OUTAGES

Protecting your business from IT outages

IT outages such as the one involving CrowdStrike are likely to occur more often in the future. Businesses can prepare for such events by quantifying their cyber risk, creating plans that minimise the downtime of critical functions, and securing effective cyber insurance coverage.

What caused the recent outage?

The outage that began on Friday, July 19, resulted from a software update defect involving cybersecurity company CrowdStrike's Falcon threat monitoring platform. According to Microsoft, 8.5 million Windows devices were affected by the content update.

Despite affecting less than 1% of all Windows machines — and not affecting Mac and Linux devices — the outage led to widespread disruption globally. Airlines cancelled thousands of flights, hospitals were forced to delay nonessential surgeries, and banking customers were unable to access their online accounts. Parametrix, a managing general agent focused on cloud services, estimates that U.S.-based Fortune 500 companies alone face $5.4 billion in losses from the outage, only a fraction of which will be insured.

How often do outages like this occur?

Widespread outages such as the one involving CrowdStrike are not everyday occurrences. They can, however, occur with some regularity, whether as a result of software errors, cyberattacks, or other causes. In June, for example, a ransomware attack involving a car dealership software provider shut down dealer systems across the U.S. for more than a week. In February, a technology outage involving a leading American wireless carrier led to 92 million phone calls being blocked over a period of at least 12 hours.

Many smaller-scale incidents often go unreported by news media and unnoticed by the general public but can have devastating impacts on individual companies.

Should businesses expect more outages going forward? Why?

Yes, they should.

The growing challenge for businesses that rely on technology to perform key operations — and a reason for many to worry about outages becoming more frequent in the future — is that technology networks are becoming increasingly complex and less transparent. Imagine, for example:

- Companies B, C, and D all rely on company A as a critical technology vendor.
- At the same time, companies B, C, and D each provide critical technology services to hundreds more companies.

- A software error or cyberattack involving vendor A shuts down companies B, C, and D — and as a result, hundreds of companies with which company A does not have any direct relationship.

In this scenario, many of the hundreds of adversely affected companies may not even be aware of company A's existence. Some of these companies may have advance plans in place to source key technology services from alternatives to companies B, C, and D in the event of a disruption… but what if a company's predetermined backup choice also relies on company A?

Do cyber insurance policies respond to technology outages?

Depending on the details of an individual loss and claim, a cyber insurance policy that includes coverage for business interruption and contingent business interruption may respond to an outage. Not every insurer, however, offers such coverage in standard cyber insurance policy forms. Businesses should work with their insurance brokers to ensure their cyber insurance policies include coverage for business interruption and contingent business interruption, with appropriate limits and sublimits to ensure protection in the event of a loss.

Are insurers concerned about the frequency of technology outages? Could this affect the availability of coverage?

Cyber insurance is currently readily available, although insurers are concerned about systemic risks related to large-scale outages and cyberattacks. Insurers have responded to these concerns by tightening war and infrastructure exclusions in policies, as well as responding to a greater level of scrutiny from reinsurers on managing systemic exposure. In addition, prospective cyber insurance buyers are now generally required to demonstrate they have a variety of cybersecurity controls in place in order to purchase coverage.

What can companies do to mitigate the potential impacts of technology outages?

A critical first step for organisations is to quantify their cyber risk. If you rely on technology to perform critical functions, it's important to understand what your downtime can look like, which companies you are dependent on to remain operational, and what your backup options are.

Given the complexity of technology networks, it's important that a company's key vendors perform their own quantification exercises. In some cases, customers may be able to contractually require vendors to take such steps, but this may depend on the size of a contract and/or the risk a specific vendor presents to a customer's business.

No company can eliminate the possibility of technology outages occurring. It is therefore vital that businesses also develop cyber incident response plans. As basic, generic, and/or outdated plans will not be useful during a crisis, it's important that organisations' written plans:

- Identify the key steps businesses must take to identify, contain, respond to, and continue operations in the event of an incident.
- Be printed, disseminated, and stored in multiple locations so they are easily accessible during an incident.
- Be tested and updated at least once a year, in conjunction with other elements of an organisation's broader business continuity plans.

For more information, contact a member of Lockton's Cyber & Technology Practice.

Name	Title	Phone	Email
Michelle Faylo	EVP, U.S. Cyber & Technology Leader	+1 816 912 6539	mfaylo@lockton.com
Lucy Scott	Partner	+44 750 694 3276	lucy.scott@lockton.com
Brendan Fitzpatrick	Privacy and Cyber Risk Consult	+1 816 381 3876	brendan.fitzpatrick@lockton.com