CrowdStrike IT outage:
Guidance for Airmic members on the CrowdStrike outage and insurance implications – Priority actions

INTRODUCTION

This note is intended to assist Airmic members in considering the insurance implications of the CrowdStrike IT outage. It has been produced in partnership with Herbert Smith Freehills. The CrowdStrike IT outage has had an extraordinary impact across the globe. Many Airmic member organisations may well have been impacted and many of those impacted will potentially suffer significant losses, including lost revenue, potential liability to customers and potentially regulatory or crime-related losses.

This note outlines the insurance cover that may be available to organisations that have been impacted by the outage (both directly and indirectly) and the steps organisations should take now to maximise their potential recoveries.

WHAT INSURANCE COVER MIGHT POLICYHOLDERS HAVE?

There are a variety of policies that might be responsive in this situation. Key classes of insurance to consider are as follows, although there may of course be others:

- Cyber insurance (or other combined coverages that include non-damage business interruption)
- Professional Indemnity ("PI") insurance / Technology Errors & Omissions ("Tech E&O") insurance
- Crime insurance
- Directors & Officers ("D&O") insurance
- Travel insurance
- Event cancellation insurance

The starting point in identifying which insurance cover is going to be responsive, is to identify the losses the organisation has suffered or may suffer.

Potential losses include:

- **Revenue losses and increased costs of working** (referred to as "business interruption" losses). These will be the immediate losses of concern for organisations.
- **Losses resulting from liability to third parties** as a result of, for example, service failures to customers, and the related costs of defending such claims (third party losses). It will likely take some time for these types of losses to materialise, as disputes including within supply chains emerge.

- **Regulatory exposure to costs or fines:**
  - **Data protection and privacy:** There is nothing to indicate this incident is malicious. However, where personal data is rendered inaccessible by an outage, that can be notifiable to data privacy regulators.
  - **Regulatory compliance:** In many sectors (for example, financial services or critical national infrastructure), operational outages can be notifiable if the effect is significant enough. Further, operational resilience issues may conceivably give rise to regulatory exposure for businesses which suffer extended downtime or recover slowly.
- **Losses resulting from crime:** it is reported that malicious actors are targeting organisations with scams in the wake of the incident, when organisations may be more vulnerable to attack as a result of, for example, the circulation of unusual communications. These could result in follow-on losses:
  i. First party losses (e.g. theft of monies in online accounts resulting from cyber security breaches or social engineering);
  ii. Regulatory investigations and fines due to security or data privacy breaches; and
  iii. Claims by impacted customers/ clients.

We look at each of these types of loss, and potentially responsive insurance, in turn, starting with the most immediate losses – business interruption losses.

(i) Business interruption losses

- Your organisation might find BI cover under standalone Cyber policies or under any other coverage that incorporates non-damage business interruption insurance.
- Traditional, damage-based, BI cover is unlikely to respond in these circumstances given there has not been any physical damage. However, cyber insurance cover often contains "non-damage" BI cover (i.e. cover that does not require there to have been physical damage to the insured's property). While it typically covers BI losses resulting from security breaches/ malicious acts (which on present information is not relevant here given CrowdStrike's public explanations), it may also provide cover for BI losses caused by more benign system outages. An example of that kind of cover would be insurance for business interruption loss resulting from the *"total or partial interruption, degradation in service or failure of the Computer System"*. Policyholders should check their cyber policy wordings to ascertain whether it is responsive to BI losses caused by system outages.
- Other factors may impact the scope of cover available. For example:
  i. Policies will typically be subject to deductibles or waiting-periods. For example, there may be a financial deductible, or losses within the first 6-24 hours of the interruption either may not be covered, or cover may only be triggered once that period has expired.
  ii. The policy may not provide cover for BI losses where the affected computer system is hosted or operated by a third-party/outside service provider (OSP), such as a cloud provider.
  iii. The period of cover may be limited to the period in which fixes might reasonably be implemented (rather than for the period until the fix was in fact implemented).

(ii)Liability to third parties

- Over the medium term, the biggest exposures for organisations, depending upon how they have been impacted by the outage, may result from third party claims and opportunistic crime. Potentially responsive policies are Cyber, PI, Tech E&O and Crime policies. For example:

    i. Claims against suppliers of IT services may, depending on the nature of the liability, contract terms and policy terms, be backed by the suppliers' own Tech E&O policies – these cover liability for errors and omissions by IT service providers in the provision of technology or professional services.

    ii. Claims by customers/clients against other service providers (for example, banks that cannot provide banking services to customers) may be backed by the service provider's PI insurance.

- For listed companies, D&O insurance may be relevant in the event that claims against directors are brought by shareholders.

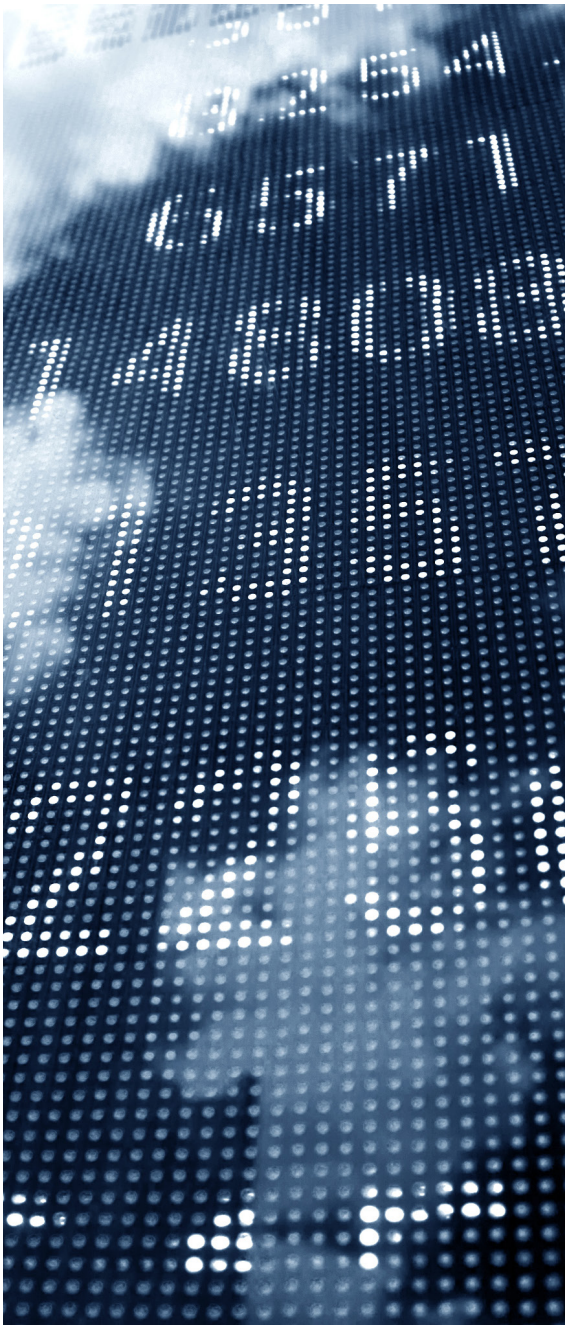
(iii) Regulatory exposures

- In addition, coverage may be available under Cyber (or other liability) insurance for costs and insurable fines if any regulatory notifications (e.g. to data privacy regulators) are required, or if regulators take any steps to investigate an organisation due to failures in operational resilience (for example if the recovery from the outage was inadequate).

- In this context, it will also be worth considering D&O insurance in the event that regulatory action is taken against directors of regulated companies due to alleged operational resilience issues.

(iv) Crime losses

- Losses due to fraud, scams or phishing may be covered under Cyber insurance for malicious acts (e.g., if there were to be a future cyber security breach) or under Crime/PI insurance (e.g., if company or customer funds are stolen) or standalone covers such as for social engineering.



We summarise the policies that might potentially respond to these different types of loss in the table below. Other policies may also respond, and policyholders ought to consider if that is the case, but the below offers a guide as to the most relevant policies:

Loss	Potentially responsive policy
Business interruption loss	Cyber policy
	Non-damage BI policy
Regulatory investigations and fines	Cyber policy
	D&O policy
Third party claims	Cyber policy
	PI policy
	Tech Errors & Omissions policy
Losses due to fraud/scams/phishing	Cyber policy
	Crime policy

In addition, depending upon your organisation, there may well be industry or sector specific insurance cover that may be responsive. Obvious examples may be Travel insurance or, as noted in the table above, Event Cancellation insurance, although there may be others.

WHAT SHOULD POLICYHOLDERS DO NEXT?

(i) Immediate steps to preserve insurance recoveries

- Identify actual or potential losses: has the business suffered business interruption losses, increased costs of working, or is it exposed to potential claims by third parties or regulatory investigations as a result of the incident?
- Review any potentially responsive policies – most obviously, any cyber coverage in the first instance.
- If there is potential cover, notify insurers of the incident promptly to attach cover.
- Preserve/retain evidence as to how events unfolded within the particular organisation, and be mindful of privilege.
- Seek any consents as appropriate (e.g. to the incurring of costs off-panel for insurers).