AN INTRODUCTION TO SILENT CYBER.

The growth of cyber exposures in recent years has led to a requirement for clarity in policy wordings around whether insurance cover would, or would not, respond to cyber-related incidents. Customers may not fully understand whether they have adequate cover for current and emerging cyber risks.

For insurers, potential cyber exposure may not have been adequately factored into premiums on some policies. And, for you as brokers, it might be difficult to explain to customers at point of sale or at claim stage which policies may or may not respond to a cyber incident.

As a result, the Prudential Regulation Authority has asked insurers to outline, in every policy, whether cyber cover is included or excluded. In addition, the Financial Conduct Authority have set an expectation that all insurers will actively manage any 'non-affirmative' cyber cover.

We have recently updated our policy wordings to set out our position more clearly on whether cover for cyber-related incidents and personal data exposure is or is not included. Our new wordings are available as part of our quote or renewal process.

Our wordings now include up to five definitions which may be used within the exclusion(s) to each policy:

- cyber attack;
- hacker (includes employees);
- computer or digital technology error (includes unintentional issues);
- social engineering;
- personal data.

The above definitions help set out the cover for (or exclusions in respect of) cyber- and personal data-related incidents under each policy wording.

Our approach

Each claim is different; whether or not the policy affords cover will be determined by the particular circumstances of the claim and the specific terms and conditions set out in your client's policy documentation (including policy limits, excesses and any endorsements).

The following are examples of cyber- or personal data-related claim scenarios and are provided as a guide only to the types of incident that our policies may, or may not, typically respond to.

Public liability (PL)

Our intent has never been to provide cover for a cyber-related incident under a PL policy.

For example, these scenarios would not be covered:

- following a data breach, your client's customer data was lost and they suffered mental anguish as a result;
- your client's customer's laptop was infected with a virus when connected to your client's company network.

Buildings, contents and other property wordings

Our intent is not to provide cover for damage to any item that is directly caused by a cyber incident, or where damage spreads digitally from one item to the next. However, we do cover subsequent damage to other covered property that arises as a result of the initial incident.

For example, this scenario would typically be covered:

- your client's digitally activated fire suppression system (e.g. water mist or deluge sprinkler), was hacked and turned on, causing damage to your client's building or contents. The damage to the buildings and contents would be covered, although we would not cover damage to the fire suppression system itself caused by the hack.

For example, this scenario would not be covered:

- your client's digital device no longer works following a cyber attack, hack or other related issue.

Management liability

Our intent is to provide cover where your client or your client's director fails to properly manage a cyber-related incident. We also provide sub-limited cover where your client's director faces personal liability in relation to a personal data claim which is the direct result of a cyber incident or that director's own unintentional error.

For example, this scenario would typically be covered:

- a claim is brought against your client's director for mismanagement following a cyber incident, due to a loss of value in the company;
- your client is investigated following a data breach which resulted from a cyber attack.

For example, this scenario would typically be covered to a sub-limit:

- your client's directors are personally investigated by the ICO following a data breach which resulted from a cyber attack.

For example, these scenarios would not be covered:

- any data recovery or forensic costs for your client following a data breach or cyber hack;
- claims against your client from data subjects whose data has been leaked following a cyber attack or hack.

Professional indemnity (PI)

Our intent is to provide cover for claims against your clients who provide technology services as part of their business activities, following a cyber-related incident where the claim results from negligence by your client.

For example, this scenario would typically be covered:

- your client maintain firewalls as part of its business activities, but its cyber security wasn't strong enough, resulting in a hack against your client's customer. We would cover claims against your client arising from their breach of duty in failing to maintain suitable firewalls.

For example, this scenario would typically be covered to a sub-limit:

- your client operates a portal for its customers. Your client mistakenly allowed its customers to be able to access other customers' information. Any resultant claims from your client's customers against your client would typically be covered by your client's PI cover to a sub-limit.

For example, these scenarios would not be covered:

- your client's system suffered a cyber attack which prevented them from completing a contract;
- your client suffered a cyber hack which resulted in confidential information being available on the dark web.

Get in touch

Updated policy summaries and summaries of change on individual risks are available, and will be sent as part of your customer's renewal documents as they move to our latest wordings. Please review your client's wordings and explain the silent cyber changes to them as part of the quote or renewal process.

Where more extensive cover for cyber incidents is required, please contact us for a quote under our award-winning CyberClear policy.

If you have any questions please contact your local underwriter.

Hiscox
22 Bishopsgate
London EC2N 4BQ
United Kingdom

T +44 (0)20 7448 6000
E enquiry@hiscox.com
www.hiscox.co.uk

21504 08/22

HISCOX