CPM

INSURANCE FOR CYBER, PRIVACY AND MEDIA RISKS

HEALTHCARE COMPANY LOSES 315k PATIENT FILES

A Canadian healthcare firm had kept a record of every patient it treated and each procedure it performed since it was founded more than 20 years ago. These records were kept in filing cabinets and eventually moved onto a computer system.

After searching several of the filing cabinets for older records, however, an employee discovered that over 300,000 paper records were missing. It was unknown whether the files were lost or stolen.

Although the loss did not result in a lawsuit and there was no legal requirement to notify affected individuals under Canadian law, the company still wished to notify clients of the loss in order to protect their brand and reputation. Unlike many other policies, CFC will cover the costs associated with voluntary breach notification.

EXPERIENCE DAY OPERATOR LEAKS CREDIT CARD DETAILS

An Edinburgh-based operator of experience days took deposits for the activities it offered over the phone and through its website. These details were then stored so that the same card could be charged again a few days before the experience day was to take place.

One of the company's employees, however, mistakenly leaked a file containing this credit card information into the public domain, exposing card details belonging to over 1,000 customers. This breach resulted in a claim for damages brought by the company's acquiring bank through provisions in their merchant agreement.

Many insurers exclude contractual liability from cyber liability insurance policies. However, our privacy liability section covers the payment of fines, penalties or contractual damages the operator would be legally obliged to pay due to a breach of privacy obligations. CFC is one of the only providers of this type of cover which is key for any company that processes and stores credit card information and as a result is subject to Payment Card Industry (PCI) security rules.

HACK ATTACK ON BLOG PUBLISHER

A large American blog publishing company held the data of several million blogs on its servers. Although it was in no way involved with the content published on these blogs, the strength and security of its servers ultimately ensured that the blogs' content was visible online.

After just a few years in operation, however, the blog publisher's servers came under attack by hackers. The attackers were not after private data or money, but rather they disagreed with the content on some of the blogs. In retaliation, they attacked the servers which hosted them hoping to disrupt the availability of the content.

Attacks such as these, because they are ideologically motivated, are often precluded from cover due to the wording of standard war and terrorism exclusions. In our CPM product we provide a specific carveback to the terrorism exclusion to ensure that cover is provided for hack attacks regardless of the attacker's motivation.

CPM

INSURANCE FOR CYBER, PRIVACY AND MEDIA RISKS

ONLINE RETAILER'S SITE CRASHES AT CHRISTMAS

For an online retailer, the weeks before Christmas are some of the most crucial in meeting income goals for the year. In fact, for one online retailer who specialised in gadgets, over 40% of annual earnings were taken in the months of November and December.

So when the gadget retailer's website was brought down for an extended period of time due to a distributed denial of service attack just three weeks before Christmas, the system downtime resulted in a much larger percentage of annual earnings being lost than the downtime would have for the same amount of time at any other point in the year.

Our CPM policy recognises that online retailers often have very seasonally affected sales and provides cover for system business interruption on an adjusted basis, rather than according to a specific formula. This ensures that clients receive exactly the right amount of cover at the time they most need it.

UNIVERSITY DISCOVERS THEFT OF PAPER RECORDS

A large American university stored a vast amount of data about students and employees both on and offline. Their paper records were stored in vast storage facilities on the university campus.

Whilst searching through the paper records, however, an employee discovered that a certain collection of files had been tampered with and several had gone missing. Upon further investigation, it was concluded that a former student had stolen the files.

Universities deal with a huge amount of personally identifiable information including names, birthdays, addresses, health records, academic records, and financial and loan information, and many of these records are stored in paper format. CPM crucially covers paper records as well as computer data in the privacy liability section of the policy.

CHARITY SUED FOR SOCIAL MEDIA CONTENT POSTED BY EMPLOYEE

Understanding that social media was becoming key in fundraising and gaining awareness for their organisation, a UK-based charity's marketing department became very active on several networks including Twitter, YouTube and Facebook. It also actively encouraged their employees to post content on these networks.

Even though the company had a fairly stringent social media policy in place, one of its employees posted defamatory content out of hours about a rival charity. The comment led to a defamation claim against the organisation.

User generated content is explicitly covered under all three major insuring clauses in the CPM policy and for this type of claim, the defamation section under the multimedia liability and advertising injury section would respond. CPM also does not limit this cover to content posted during the course of regular business activities, but includes content disseminated after hours and for non-business related activities.