

Często zadawane pytania (FAQ)

Poniższe pytania i odpowiedzi zostały opracowane, aby pomóc Państwu w zrozumieniu produktu.

Czy warto kupić polisę Leadenhall Cyber?

Należy rozważyć zawarcie ubezpieczenia Cyber, ponieważ:

- ryzyko awarii systemu informatycznego oraz wycieku lub utraty danych (cyfrowych i innych) - dotyczy każdego,
- ryzyko to nie jest objęte innymi polisami,
- to jedyna polisa pokrywająca wszystko co istotne: kary - w tym nakładane przez GIODO i operatorów kart płatniczych, koszty obrony oraz koszty naprawy systemów IT, utracone zyski, a w końcu odpowiedzialność cywilną, w tym także wobec własnych pracowników.

Czym jest polisa Cyber?

To najszybciej rozwijająca się gałąź ubezpieczeń na świecie, pokrywająca w jednej polisie:

- odpowiedzialność cywilną za wyciek lub utratę danych,
- koszty obrony oraz kary w przypadku naruszenia prawa do prywatności,
- odpowiedzialność cywilną i koszty reakcji w razie naruszenia bezpieczeństwa własnych komputerów skutkujące usunięciem lub zmianą danych, wysłaniem szkodliwego wirusa, odmową wykonania należnej komuś usługi itp.

Dodatkowo polisa może obejmować:

- odpowiedzialność cywilną za naruszenie dóbr osobistych i praw własności intelektualnej w przekazie cyfrowym
- koszt odtworzenia danych i zysk utracony przez Ubezpieczonego.

Termin Cyber kojarzy się z zagrożeniem wyłącznie 'elektronicznym' lub 'internetowym' dotyczącym danych cyfrowych i systemów IT. W rzeczywistości stanowi znacznie szerszą ochronę, obejmując ujawnienie lub utratę danych poufnych, korespondencji i dokumentów w innych formatach - na papierze i nośnikach analogowych.

Assistance i koszty reakcji

Polisa Cyber zapewnia Ubezpieczonemu dostęp do specjalistycznego 'know how' współpracujących z Lloyd's agencji PR, ekspertów ds. ochrony danych oraz systemów IT i kryminalistyki informatycznej, prawników z zakresu prawa medialnego, prawa pracy, prawa telekomunikacyjnego oraz ochrony danych osobowych.

Polisa Cyber zapewnia assistance pozwalający Ubezpieczonemu zareagować optymalnie i niezwłocznie po zidentyfikowaniu zdarzenia. To szczególnie ważne dla podmiotów małych i średnich, które nie dysponują zasobami niezbędnymi do samodzielnego uporania się Cyber zagrożeniem.

Kto ubezpiecza ryzyko Cyber?

Polisa Leadenhall Cyber jest w 100% uplasowana w londyńskim Lloyd's. Odszkodowania gwarantuje syndykat specjalizujący się w tym ryzyku. Wszystkie syndykaty legitymują się ratingami A, A+ lub AA-, przyznanymi Lloyd's przez trzy największe agencje ratingowe: Standard & Poors, A.M. Best i Fitch.

Lloyd's jest światowym liderem ubezpieczeń Cyber. Z publikowanych przez niego informacji wynika, że liczba polis Cyber i łączna kwota roszczeń do nich wzrośnie w najbliższych latach wielokrotnie, a rynek tych ubezpieczeń przekroczy 50 mld £ składki. To obrazuje trwającą właśnie eksplozję zagrożeń oraz świadomości ryzyk związanych z bezpieczeństwem informacji.

Lloyd's jest najstarszą instytucją ubezpieczeniową świata, działająca nieprzerwanie od ponad 325 lat. Kilkadziesiąt miliardów funtów aktywów oraz zbieranej corocznie składki, czynią go także jedną z największych.

Leadenhall Polska S.A. jest coverholderem rynku Lloyd's zarejestrowanym pod numerem 10993CTM.

Jako coverholder posiada pełnomocnictwa do zawierania i wykonywania umów ubezpieczenia w imieniu Lloyd's

Co pokrywa Sekcja A polisy - Ubezpieczenie odpowiedzialności cywilnej i kosztów obrony w sprawach o naruszenie prywatności?

Leadenhall Cyber definiuje 'prywatność' pełniej niż wynika to z Ustawy o ochronie danych osobowych.

Ubezpieczenie obejmuje nie tylko odpowiedzialność za nielegalny wyciek danych osobowych (w tym danych wrażliwych) oraz firmowych danych poufnych, lecz także odpowiedzialność wynikającą z wszelkiego naruszenia prawa do prywatności, prawa do wizerunku itp.

To ważne, bo ujawnione dane mogą nie spełniać ustawowych definicji danych osobowych – dlatego Leadenhall Cyber rozszerza ochronę tak, by pokryć tę lukę.

Co pokrywa Sekcja B polisy - Kary za naruszenie prywatności?

Zapewnia zwrot kar i grzywien nałożonych w konsekwencji postępowań regulacyjnych o naruszenie prywatności. Dotyczy to także naruszenia polskiego lub zagranicznego prawa dotyczącego ochrony danych, w szczególności Ustawy o ochronie danych osobowych - w tym kar nałożonych przez GIODO. Pokryte są także koszty obrony w takich postępowaniach.

Co pokrywa Sekcja C polisy - Koszty naruszenia bezpieczeństwa informacji?

Zapewnia zwrot wydatków poniesionych na skutek naruszenia bezpieczeństwa danych osobowych - tak klientów, jak i pracowników Ubezpieczonego. Naruszenie danych może polegać na ich utracie, ujawnieniu, uszkodzeniu, kradzieży, wycieku etc.

Pokryte są koszty:

- agencji Public Relations (PR) wynajętych do zapobieżenia lub ograniczenia szkód w wizerunku,
- badań z zakresu kryminalistyki informatycznej oraz obsługi prawnej służącej ustaleniu obowiązków Ubezpieczonego wynikających z przepisów o ochronie danych,
- wymaganego prawem powiadomienia dotkniętych zagrożeniem klientów
- monitorowania i podtrzymania poziomu ich zaufania

Polisa może pokryć koszty powiadomienia klientów również wtedy, gdy Ubezpieczony nie mając takiego obowiązku uzna, że zmniejszy tym szkody na wizerunku. Wymaga to jednak uprzedniej zgody Ubezpieczyciela.

Co pokrywa Sekcja D polisy - Odpowiedzialności cywilna i koszty obrony w sprawach o naruszenie bezpieczeństwa informacji?

Zakres obejmuje odpowiedzialność za:

- brak możliwości korzystania z systemu IT Ubezpieczonego przez klientów i inne uprawnione osoby trzecie,
- bezprawny dostęp do tego systemu, jego wykorzystanie lub dopuszczenie do fałszywej z niego komunikacji (np. 'phishing') umożliwiające zainfekowanie, kradzież, wykasowanie lub uszkodzenie danych, bądź umożliwiające atak na system lub usługę sieciową osoby trzeciej w celu uniemożliwienia ich działania,
- dopuszczenie do rozsyłania wirusa z systemu IT Ubezpieczonego

* Phishing – wyludzanie internetowe poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której rzekomo informacje te są pilnie potrzebne.

Co pokrywa Sekcja F polisy - Cyber wymuszenie?

Zapewnia środki finansowe na przeciwdziałanie celowemu:

- wprowadzeniu szkodliwego wirusa do systemu IT Ubezpieczonego,
- przerwaniu pracy tego systemu,
- zniekształceniu, niszczeniu lub rozpowszechnianiu danych osobowych lub poufnych informacji firmowych przez działającą umyślnie osobę trzecią.

Obejmuje:

- Koszty oceny tego zagrożenia i adekwatnej reakcji na nie (honoraria specjalistów ds. zarządzania kryzysowego),
- Refundację wymuszonej oraz uzasadnionej ekonomicznie płatności na rzecz osoby faktycznie mogącej dokonać powyższych czynów.

Co pokrywa Sekcja G polisy - Utracony zysk i koszty odtworzenia danych?

Zwraca utracony zysk i koszty poniesione na skutek naruszenia bezpieczeństwa prowadzącego do:

- zakłócenia pracy systemu IT lub jego awarii,
- braku możliwości dostępu i korzystania z niego przez uprawnione osoby trzecie.

Pokrywa także koszty przywrócenia lub odtworzenia zasobów cyfrowych (ale nie sprzętu komputerowego) do stanu bezpośrednio przed szkody.

Definicja **systemu IT** obejmuje nie tylko systemy znajdujące się bezpośrednio pod kontrolą Ubezpieczonego, lecz także będące pod kontrolą **dostawcy usługi** z którym Ubezpieczony ma umowę przechowania lub przetwarzania danych cyfrowych.

Wariant dostępny tylko, gdy Ubezpieczony posiada plan zachowania ciągłości działalności w razie naruszenia bezpieczeństwa informacji tzw. Disaster Recovery Plan.

Co wyróżnia polisę Leadenhall Cyber?

Leadenhall Cyber wyróżnia obszerny zakres ochrony wynikający z niezwykle pojemnych **definicji** oraz czytelnego katalogu **wyłączeń**.

Maksymalnie szeroko definiuje ona najważniejsze dla zakresu ochrony pojęcia: naruszenie prywatności, system informatyczny oraz zawartość multimedialna.

Rezygnując z wymogu wypełniania skomplikowanego wniosku, umożliwiliśmy natychmiastowe uzyskanie oferty. Zawarcie on-line polisy Leadenhall Cyber wymaga jedynie podania kilku podstawowych informacji o Ubezpieczonym i jego systemie IT.

Czy małe i średnie podmioty potrzebują polisy Cyber?

Raport Zagrożeń Bezpieczeństwa w Internecie 'Symantec 2014' donosi, że w 2013 małe przedsiębiorstwa **były celem 30%** wszystkich cyber ataków zmierzających do wyłudzenia poufnych informacji.

Szacuje się, że około **40% wszystkich wycieków** danych dotyczy podmiotów **zatrudniających poniżej 100 osób***.

22% respondentów badania 'Kradzież tożsamości' przeprowadzonego w 2014 roku przy współpracy merytorycznej Biura Informacji Kredytowej (BIK), było narażonych na utratę danych osobowych. 18% przyznało, że sytuacja taka dotyczyła ich bliskich. Łącznie problem kradzieży tożsamości dotknął aż 40% badanych.

62% ankietowanych nie niszczy dokumentów w sposób uniemożliwiający identyfikację danych. Dotyczy to nawet wyciągów bankowych, potwierdzeń przelewów, rachunków i innych dokumentów księgowych.

Według amerykańskich badań **60% firm**, które padły ofiarą cyber ataku, **zniknęło z rynku w ciągu kolejnych 6** miesięcy. Nie jest to zaskoczeniem wzięwszy pod uwagę, że średnia strata poniesiona w wyniku cyber ataku wyniosła 3,5 mln USD, a kwota ta wzrosła o 15% w ciągu ostatnich 12 miesięcy.

O ile o wyciekach danych z wielkich korporacji, przedsiębiorstw państwowych i organizacji rządowych czytamy w nagłówkach gazet, to właśnie małe przedsiębiorstwa są najbardziej zagrożone ich skutkami.

Dysponując znikomymi budżetami, ograniczonymi zasobami ludzkimi oraz większymi lukami w procedurach i systemach IT, małe firmy powinny być szczególnie zainteresowane zabezpieczeniem ryzyka polisą Cyber.

* Za Verizon Communications – jednym z największych dostawców usług telekomunikacyjnych takich jak telefonia komórkowa, szerokopasmowy dostęp do Internetu i telewizja kablowa. Notowany na giełdzie NYSE, wchodzi w skład indeksu Dow Jones 30.

Czy polisa Cyber jest potrzebna, gdy obszar handlu elektronicznego jest zlecany 'na zewnątrz'?

Przez obszar handlu elektronicznego w szczególności rozumiemy obsługę płatności i przechowywanie danych o klientach i transakcjach.

Obowiązki prawne związane z ochroną danych oraz poinformowanie klientów o ich wycieku są wyłącznym obowiązkiem przedsiębiorcy. Nie zastąpią go w tym zakresie dostawcy usług.

Zlecenie podwykonawcom istotnych biznesowo działań, takich jak obsługa płatności, przechowywanie danych, hosting stron www itp., może jedynie ograniczyć ryzyko ciążące na Ubezpieczonym. Jednak to postanowienia umów zawieranych z jego klientami i podwykonawcami wyznaczają zakres odpowiedzialności stron w poszczególnych przypadkach.