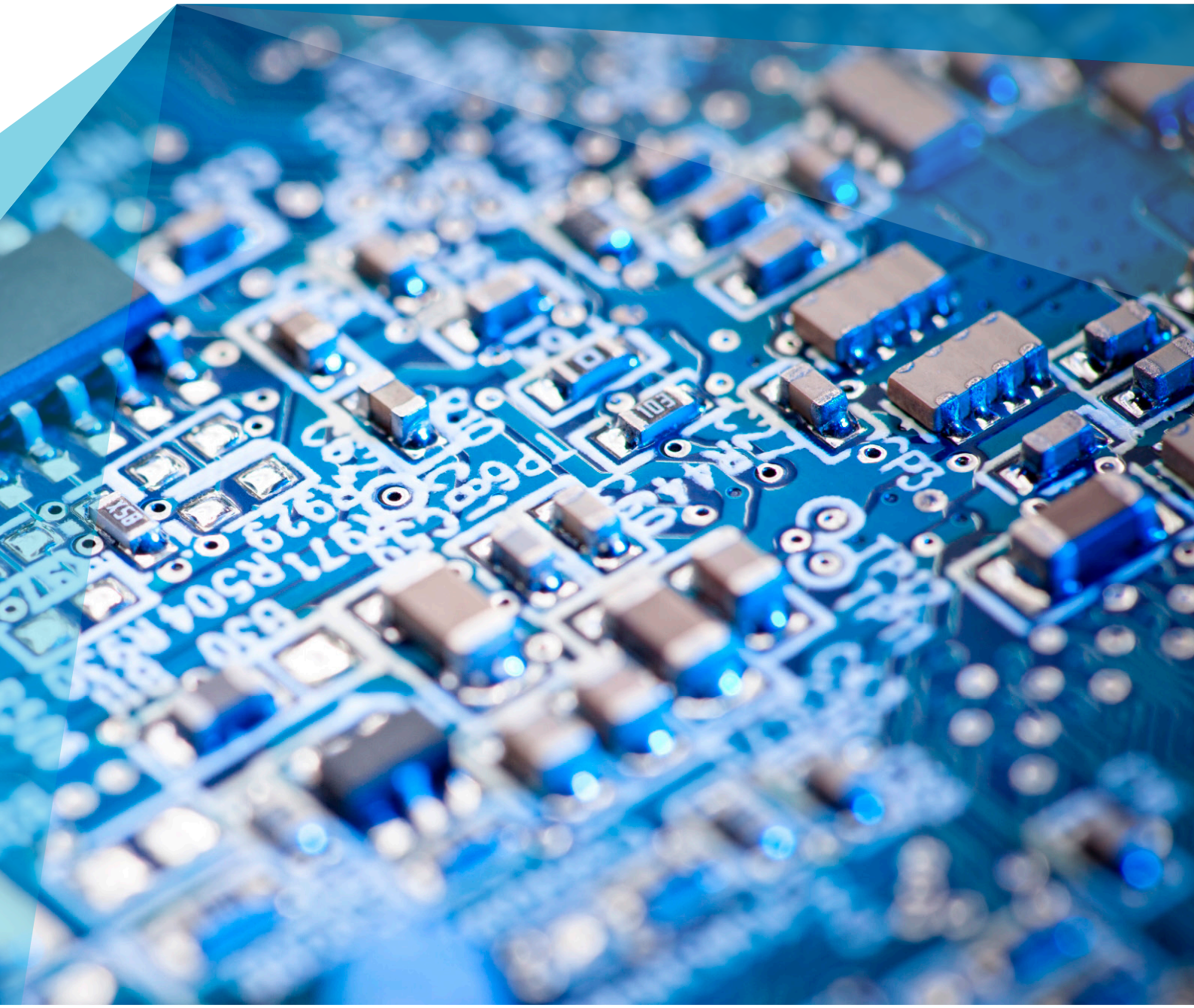
MARSH

ZARZĄDZANIE RYZYKIEM CYBERNETYCZNYM
NASZE ROZWIĄZANIA



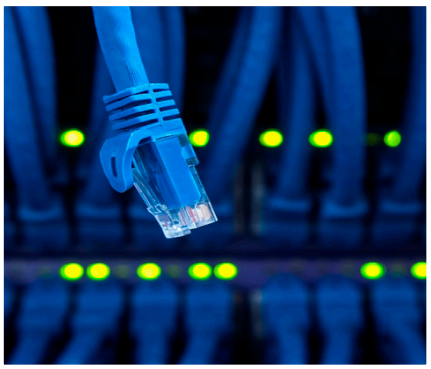
SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

ODPOWIEDZIALNOŚĆ PRAWNA WOBEC OSÓB TRZECICH ZA NARUSZENIE BEZPIECZEŃSTWA SIECI KOMPUTEROWEJ

ODPOWIEDZIALNOŚĆ PRAWNA WOBEC OSÓB TRZECICH ZA UTRATĘ DANYCH OSOBOWYCH

POSTĘPOWANIA REGULACYJNE I ŚLEDZTWA



UTRATA ALBO ZNISZCZENIE DANYCH LUB INFORMACJI

UTRATA ZYSKU WSKUTEK ATAKU CYBERNETYCZNEGO

DODATKOWE KOSZTY ZWIĄZANE Z ODPOWIEDZIĄ NA ATAKI CYBERNETYCZNE

UTRATA LUB NARUSZENIE REPUTACJI

CYBER-WYMUSZENIA

CYBER-TERRORYZM

ZARZĄDZANIE RYZYKIEM CYBERNETYCZNYM
NASZE PODEJŚCIE

Konsekwencje wystąpienia ryzyk cybernetycznych mogą negatywnie wpłynąć nie tylko na firmę, lecz również członków jej zarządu, klientów, dostawców oraz innych interesariuszy. Przedsiębiorstwa, rozumiejąc skalę zagrożenia, które niesie za sobą coraz większa zależność od systemów informacyjnych, muszą zadbać o adekwatną ochronę przed ryzykiem cybernetycznym.

Aby osiągnąć ten efekt, firma musi odpowiedzieć na trzy podstawowe pytania:

- Jakie zagrożenia cybernetyczne towarzyszą prowadzonej działalności?
- Jakie mogą być finansowe konsekwencje wystąpienia wskazanych zagrożeń?
- Do jakiego stopnia ryzyko może zostać przeniesione na rynek ubezpieczeniowy?

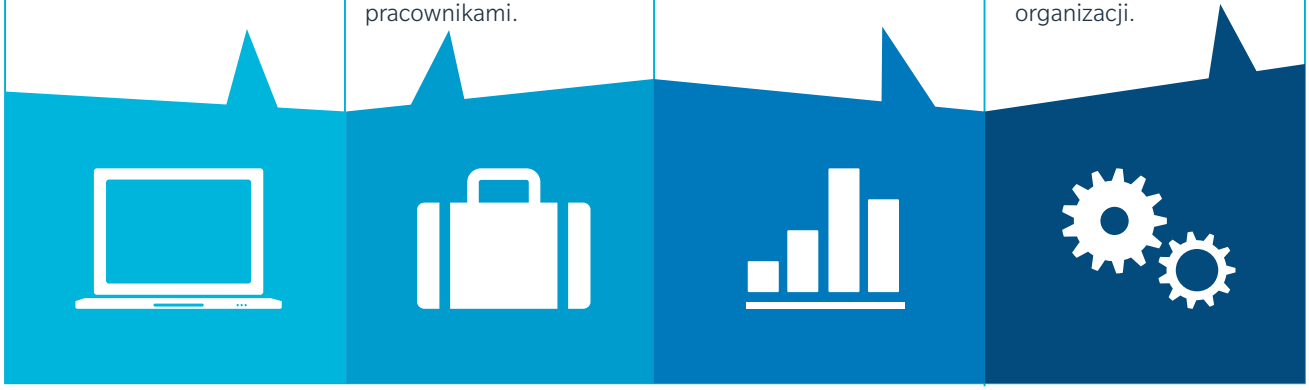
Usługi doradcze oferowane przez Marsh pozwalają na kompleksową ocenę potrzeb ubezpieczeniowych firmy - nasi konsultanci ocenią czy w świetle zidentyfikowanego profilu ryzyka niezbędne jest jego przeniesienie na rynek ubezpieczeniowy oraz w jaki sposób powinno zostać ono zaaranżowane.

Rekomendacje opracowane na podstawie przeprowadzonych przez nasz Zespół analiz mogą wpłynąć na poprawę systemu zarządzania ryzykiem cybernetycznym i tym samym umożliwić uzyskanie korzystniejszego pod względem kosztu i zakresu pokrycia ubezpieczeniowego.

Poniżej przedstawiamy metodologię Marsh - kompleksowe podejście do analizy, identyfikacji i zarządzania ryzykiem cybernetycznym.

CEL: Optymalizacja strategii finansowania ryzyka cybernetycznego - dostosowanie programu ubezpieczeniowego do profilu ryzyka organizacji.

USŁUGI DORADCZE		OCHRONA UBEZPIECZENIOWA	
AUDYT ZGODNOŚCI Z NORMĄ ISO 27001	WSPARCIE TRANSFERU RYZYKA CYBERNETYCZNEGO	AUDYT POLIS	ARANŻOWANIE OCHRONY I OBSŁUGA
Audyt zgodności z międzynarodową normą ISO 27001 standaryzującą systemy zarządzania bezpieczeństwem informacji.	Oszacowanie finansowych konsekwencji potencjalnych incydentów cybernetycznych, w oparciu o scenariusze szkodowe i warsztaty z kluczowymi pracownikami.	Porównanie zidentyfikowanych ekspozycji z dotychczasowym pokryciem ubezpieczeniowym.	Opracowanie optymalnych rozwiązań finansowania ryzyka. Plasowanie w oparciu o zidentyfikowane potrzeby ubezpieczeniowe organizacji.



AUDYT ZGODNOŚCI Z NORMĄ ISO 27001

Pierwszy etap współpracy obejmuje szczegółowy audyt zgodności z wymaganiami międzynarodowej normy ISO 27001, standaryzującej systemy zarządzania bezpieczeństwem informacji w organizacjach.

Nasz Zespół przeprowadzi identyfikację i szczegółową analizę podatności organizacji na zagrożenia cybernetyczne, która obejmie takie obszary jak np.: zarządzanie systemami i sieciami, kontrola dostępu, organizacja bezpieczeństwa informacji czy zarządzanie ciągłością działania.

Konsultanci Marsh, poza oceną skuteczności przewidzianych oraz zaimplementowanych w organizacji zabezpieczeń technicznych i organizacyjnych, wskażą niezbędne działania korygujące oraz kierunek optymalizacji systemu zarządzania bezpieczeństwem informacji.

Wynikiem zaangażowania Marsh jest Raport z Oceny Ryzyka w Zakresie Bezpieczeństwa Informacji, który dostarczy informacji na temat:

- Podatności przedsiębiorstwa na incydenty w zakresie bezpieczeństwa informacji.
- Efektywności przewidzianych zabezpieczeń i stopnia ich wdrożenia w organizacji.
- Możliwości doskonalenia w zakresie poufności, integralności i dostępności informacji (rekomendacje poprawy ryzyka).
- Zgodności prowadzonych działań z wymaganiami normy ISO 27001 oraz przepisami warunkującymi przetwarzanie informacji (m.in.: ochrony danych osobowych, ochrony informacji niejawnych).

Jeżeli Zespół Marsh potwierdzi potrzebę zaaranżowania pokrycia ubezpieczeniowego dla ryzyka cybernetycznego, stworzony raport będzie mógł zostać użyty w celu zaaranżowania ochrony i potencjalnie przyczyni się do uzyskania atrakcyjniejszych ofert ubezpieczeniowych.

WSPARCIE TRANSFERU RYZYKA CYBERNETYCZNEGO

Po przeprowadzeniu audytu zgodności z normą ISO 27001 Marsh oceni stopień w jakim konieczne jest przeniesienie ryzyka na rynek ubezpieczeniowy. Celem Wsparcia Transferu Ryzyka Cybernetycznego jest oszacowanie finansowych konsekwencji potencjalnych incydentów cybernetycznych.

Analiza zostanie przeprowadzona na bazie warsztatów z kluczowymi pracownikami firmy, przy użyciu zbioru scenariuszy szkodowych, opracowanych w oparciu o naszą wiedzę i doświadczenie Marsh. Poszczególne prace i zadania zostaną dostosowane do branży i profilu działalności organizacji, przy uwzględnieniu jej dotychczasowej historii szkodowej.

Konsultanci Marsh wskażą zagrożenia o charakterze cybernetycznym, których realizacja może nieść znaczące (nieakceptowalne) dla przedsiębiorstwa konsekwencje finansowe. Nasza metodologia umożliwi określenie scenariuszy szkodowych, których wystąpienie może wpłynąć na poufność, integralność i dostępność posiadanych danych lub skutkować naruszeniem obowiązujących przepisów o ich ochronie. Zweryfikowane zostaną także takie kwestie jak np. zależności organizacji of dostawców systemów teleinformatycznych (ICT), czy odpowiedzialność organizacji wynikająca ze zobowiązań umownych.

Nasze działania pozwolą na ocenę zdolności organizacji do przyjęcia finansowych skutków incydentów cybernetycznych oraz umożliwią określenie spodziewanego poziomu szkód w warunkach normalnych (*Normal Loss Expectancy*) i maksymalnej prawdopodobnej szkody (*Maxiumum Foresseable Loss),* wynikających z materializacji ryzyka cybernetycznego.

Nasi Konsultanci zidentyfikują zagrożenia cybernetyczne, których realizacja zagraża misji i celom organizacji, a wyniki analizy zostaną wykorzystane aby określić optymalny program ubezpieczeniowy.

OCHRONA UBEZPIECZENIOWA
LUKI W TRADYCYJNYCH POLISACH

Ubezpieczenie cyber ryzyk może wypełnić wiele luk w tradycyjnych ubezpieczeniach, jak również zapewnić pokrycie dla strat bezpośrednich oraz ochronę przed ryzykiem odpowiedzialności związanej z wykorzystywaniem technologii i danych w codziennej działalności. Zakres polis cyber jest elastyczny, dzięki czemu program może zostać dostosowany do faktycznych, kluczowych ekspozycji na ryzyko.

Kategoria	Charakter straty związanej z Cyber ryzykiem/utratą informacji poufnych i naruszeniem danych osobowych	Rodzaj ubezpieczenia					Szeroka polisa Cyber
		Mienia/ elektroniki	OC	od ryzyka terroryzmu	OC zawodowa	od ryzyka sprzenie-wierzenia	
Ochrona aktywów elektronicznych	Zniszczenie, uszkodzenie lub kradzież informacji/ danych elektronicznych w wyniku naruszenia systemu bezpieczeństwa komputerów lub sieci komputerowych.						
Utrata zysku	Utrata zysku/przychodów w wyniku przerwy w działalności systemu komputerowego wskutek naruszenia systemu bezpieczeństwa informatycznego.						
	Utrata zysku/przychodów w wyniku przerwy w działalności systemu komputerowego spowodowanej błędem pracownika.						
Odpowiedzialność za ujawnienie danych	Odpowiedzialność wynikająca z nieuprawnionego ujawnienia danych osobowych.						
	Koszty poniesione na wymagane przez przepisy prawa informowanie osób poszkodowanych o fakcie ujawnienia ich danych.						
	Koszty obrony związane z postępowaniami regulacyjnymi wynikającymi z naruszenia prawa ochrony danych osobowych.						
	Pokrycie kar nałożonych w wyniku nieautoryzowanego udostępnienia informacji z kart kredytowych/debetowych.						
Wymuszenia	Groźby lub wymuszenia związane z ujawnieniem informacji poufnych lub naruszeniem bezpieczeństwa informatycznego.						
Odpowiedzialność za bezpieczeństwo sieci	Odpowiedzialność za szkody osób trzecich wskutek błędów w zabezpieczeniu komputerów lub sieci.						
	Odpowiedzialność wynikająca z wprowadzenia złośliwego oprogramowania lub wirusa wskutek błędów zabezpieczeniu komputerów lub sieci.						
	Odpowiedzialność wynikająca z uniemożliwienia autoryzowanego dostępu do systemów komputerowych spowodowanego błędnym działaniem systemu bezpieczeństwa komputerów lub sieci.						
Działalność multimedialna	Odpowiedzialność za treści zawarte na stronie internetowej firmy, które mają charakter zniesławiający/obraźliwy.						
	Odpowiedzialność za treści zawarte na stronie internetowej firmy, które naruszają prawa intelektualne osób trzecich, z wyłączeniem patentów oraz tajemnic handlowych.						
	Odpowiedzialność wynikająca z wprowadzających w błąd publikacji lub oświadczeń zawartych na stronach internetowych firmy.						

Luki w pokryciu - wybrane polisy ubezpieczeniowe.

OCHRONA UBEZPIECZENIOWA
PROCES ARANŻOWANIA POLISY

Po przeprowadzeniu opisanych analiz, nasz Zespół zaaranżuje kompleksową ochronę ubezpieczeniową dla zidentyfikowanych ryzyk cybernetycznych. Poniżej przedstawiamy ramowy proces plasowania polisy.

W procesie wyceny przedmiotowego ubezpieczenia najistotniejszymi kwestiami są ilości przechowywanych danych wrażliwych (dane osobowe, numery kart kredytowych, itp.) oraz wrażliwości na ryzyko utraty zysku w konsekwencji ataków / awarii systemów. Ubezpieczenie od zagrożeń cybernetycznych to przystępna cenowo i przewidywalna inwestycja w ochronę firmy na wypadek wystąpienia incydentu cybernetycznego.

Na polskim rynku ubezpieczenia cyber ryzyka znajdują się w ofercie coraz większej liczby ubezpieczycieli - ofert ochrony poszukujemy również na rynku londyńskim, specjalizującym się w tego typu rozwiązaniach.

KONTAKT

Anna Pluta
tel.: +48 (22) 456 42 06
e-mail: anna.pluta@marsh.com

Paweł Wojskowicz
tel.: +48 (22) 456 42 62
e-mail: pawel.wojskowicz@marsh.com

Krzysztof Wrzesień
tel.: +48 667 800 034
e-mail: krzysztof.wrzesien@marsh.com