CYBER GUARD

PRZEWODNIK PO PRODUKCIE

COLONNADE
A FAIRFAX COMPANY

JAKIE SĄ MOŻLIWOŚCI SPRZEDAŻY?

ZMIANY W PRAWIE

Regulacje krajowe i międzynarodowe, takie jak Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO) stawiają nowe wymogi i zmieniają prawne postrzeganie przetwarzania danych i odpowiedzialności z tym związanej. Ubezpieczenie ryzyk cybernetycznych jest obecnie najlepszym rozwiązaniem w zakresie ubezpieczeniowej odpowiedzi na nowe regulacje.

BRAKI W OCHRONIE

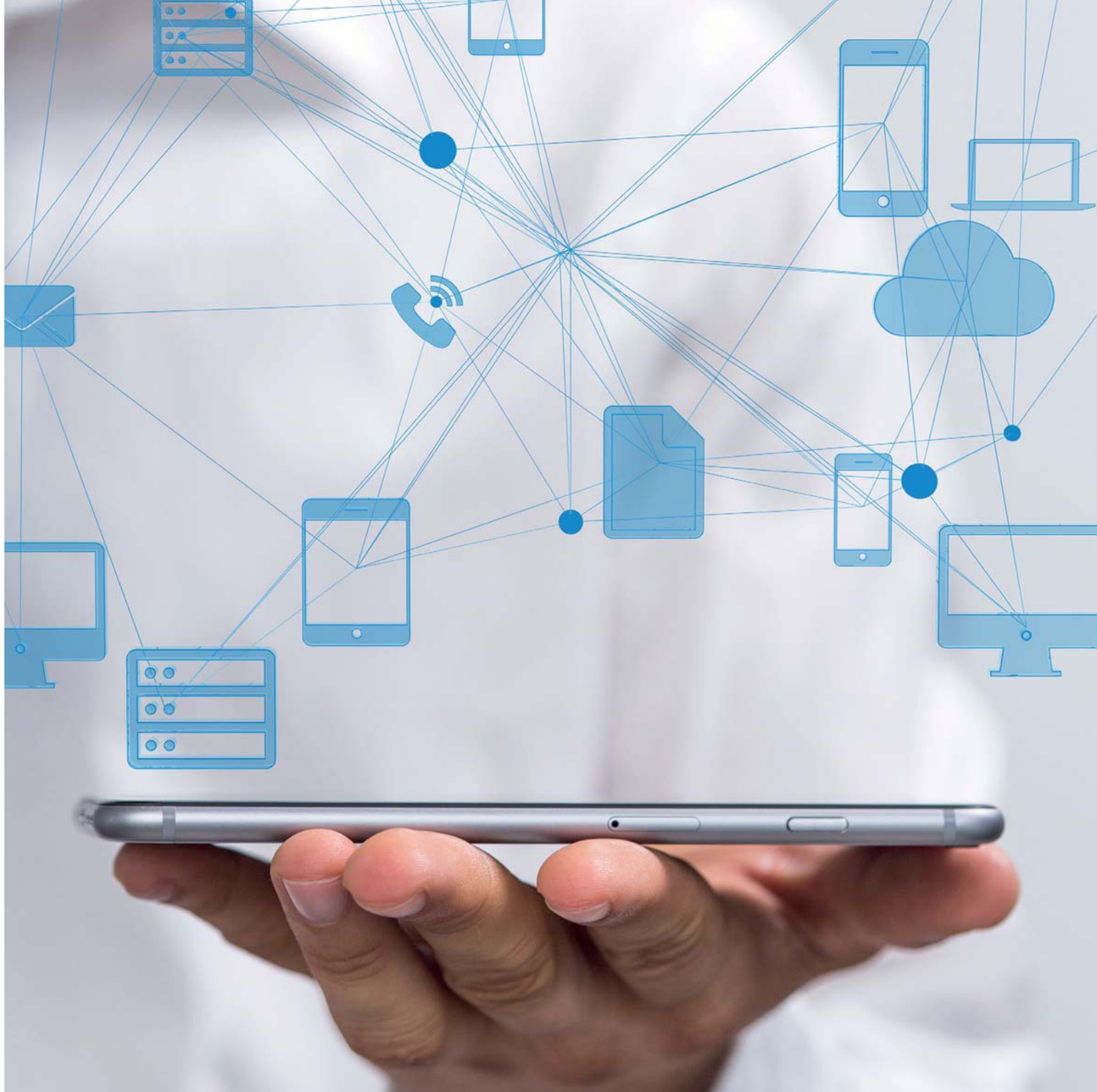
Zagrożenia cybernetyczne nie tylko otwierają listę najistotniejszych rodzajów ryzyka według risk managerów, ale również charakteryzują się jednym z najniższych stopni ochrony. Wskazuje to na duże braki w ochronie ubezpieczeniowej.

JASNO ZDEFINIOWANE RYZYKO

Mimo obaw związanych z zagrożeniami cybernetycznymi, przedsiębiorstwa nie są świadome konkretnych rodzajów ryzyka, na jakie są narażone. Ten przewodnik po produkcie pomaga w jasny sposób określić klientowi główne źródła ryzyk cybernetycznych oraz przedstawić szeroki wachlarz ryzyk objętych ochroną.

SZKODY CYBERNETYCZNE W POLSCE

- kampanie malware atakujące przedsiębiorców bez względu na branżę (Wannacry oraz Petya, maj-czerwiec 2017 r.)
- wycieki danych klientów instytucji finansowych. Hakerzy sprzedający dane klientów 4 polskich banków po 3 zł za rekord (wrzesień 2017 r.)
- kradzież danych przez pracowników call center i firmy telekomunikacyjnej (wrzesień 2017 r.)
- zagraniczny program antywirusowy, który był wykorzystywany do włamywania się i wykradania informacji z systemów użytkowników antywirusa na całym świecie (wrzesień 2017 r.)
- wyciek adresów e-mail klientów banku poprzez umieszczenie wielu odbiorców w polu CC (DW) zamiast BCC (UDW) (wrzesień 2017 r.)
- wyciek 11 000 CV studentów jednego z polskich uniwersytetów (czerwiec 2017 r.)



KIM SĄ KLIENCI DOCELOWI I DLACZEGO

PRZEDSIĘBIORSTWA PRODUKCYJNE

Firmy produkcyjne potrzebują ubezpieczenia z powodu przetwarzania danych pracowników, przetwarzania informacji handlowych kontrahentów, stopnia cyfryzacji przedsiębiorstwa oraz stopnia uzależnienia od systemów informatycznych.

UNIWERSYTETY

Uniwersytety i inne szkoły wyższe są narażone na ryzyko ponieważ:

- gromadzą dużo poufnych informacji (numery kart kredytowych kandydatów, wyniki osiągane w nauce, wyniki prowadzonych badań oraz dane dotyczące stanu zdrowia),
- przechowują dane na urządzeniach przenośnych,
- korzystają ze zdalnego dostępu do zasobów sieci,
- korzystają z mediów społecznościowych
- używają oprogramowania do zarządzania finansami uczelni.

FIRMY HANDLOWE

Firmy te:

- przechowują informacje o klientach, w tym numery kart kredytowych i debetowych (ryzyko skimmingu),
- są zobowiązane do przestrzegania przepisów prawnych oraz Standardów Bezpieczeństwa Danych Branży Kart Płatniczych (PCI DSS – Payment Card Industry Data Security Standards),
- mogą paść ofiarą hakerów (blokady stron sklepów internetowych).

HOTELARSTWO I TURYSTYKA

Hotele i branża turystyczna ponoszą odpowiedzialność za bezpieczeństwo i zachowanie poufności danych dotyczących rezerwacji dokonywanych w Internecie. Są także narażone na:

- na ryzyko ataków typu „Denial of Service”,
- kopiowanie kart kredytowych (skimming),
- włamania do systemów płatniczych,
- utratę informacji o kartach kredytowych,
- narażenie reputacji firmy w razie incydentu.

TELEKOMUNIKACJA

Cała branża jest zobowiązana do przestrzegania Dyrektywy unijnej i spełnienia wymogów PCI DSS. Mogą na niej ciążyć duże koszty (w tym roszczenia stron trzecich, grzywny i kary) i utrata reputacji w przypadku ataku cybernetycznego. Firmy telekomunikacyjne są także narażone na wirusa oddziałującego na infrastrukturę publiczną.

PRZEDSIĘBIORSTWA UŻYTECZNOŚCI PUBLICZNEJ

Przedsiębiorstwa potrzebują ochrony ze względu na:

- zdalne sterowanie i zdalne systemy monitoringu,
- ryzyko związane z szantażami i atakami na sieci infrastruktury krajowej,
- problemy z oprogramowaniem serwerowym,
- gromadzenie danych osobowych dotyczących transakcji kartami kredytowymi,
- konieczność spełnienia wymogów PCI DSS.

INSTYTUCJE FINANSOWE

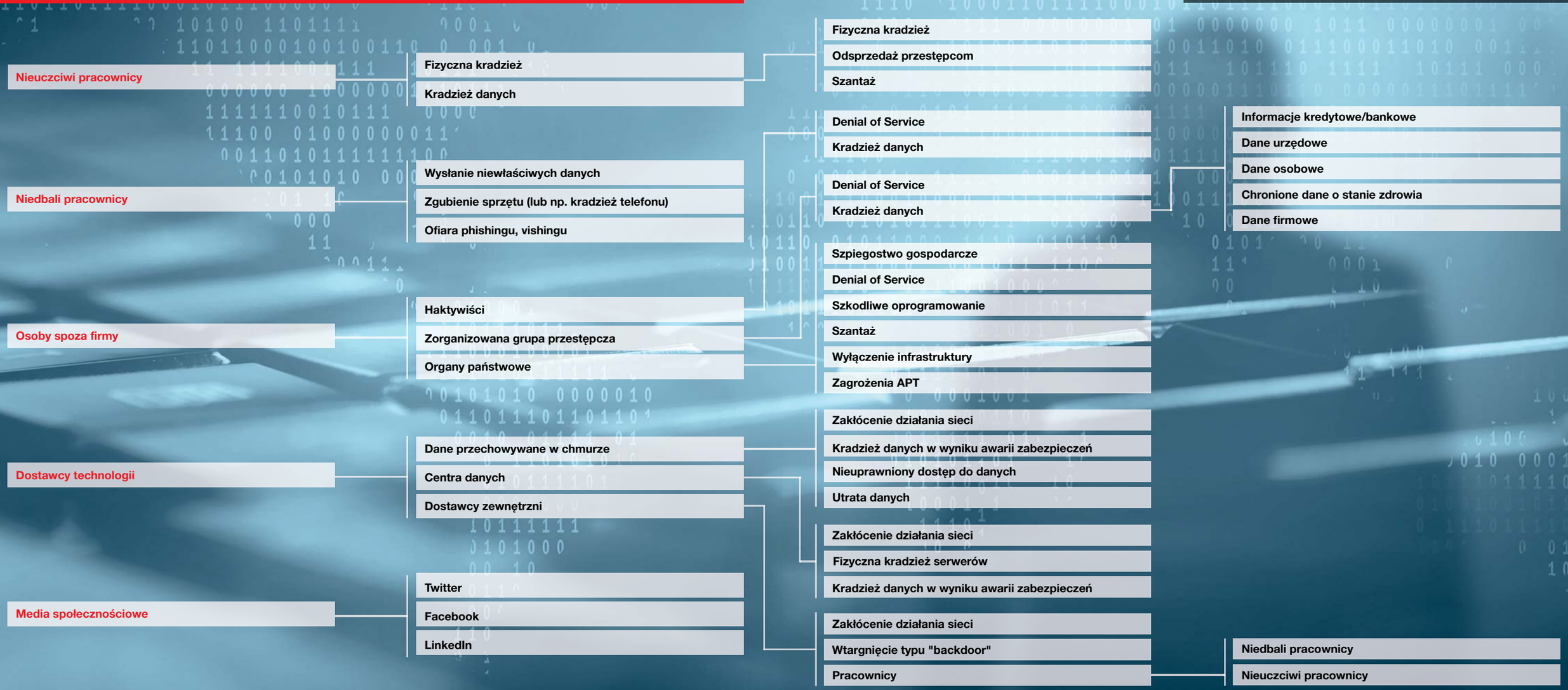
Jedne z najczęściej atakowanych przez hakerów firm przechowują ważne dane osobowe, są podatne na nowe zagrożenia i na coraz więcej ataków typu „Denial of Service”.

SPRZEDAŻ UBEZPIECZEŃ CYBER GUARD NOWYM KLIENTOM

PYTANIA I ARGUMENTY	UWAGI
Wiele firm zgłasza obawy związane z zagrożeniami cybernetycznymi. Czy rozumieją jednak, z jakimi dokładnie zagrożeniami mają do czynienia, aby móc się przed nimi zabezpieczyć?	Ryzyka, na które narażone są firmy ewoluują i stają się coraz bardziej złożone: hakerzy, złośliwe oprogramowanie, nieuczciwi pracownicy, ich zaniedbania, haktywiści, nieadekwatny poziom kontroli ze strony działu IT, błędy pracownicze... CYBER GUARD zapewnia wsparcie merytoryczne w przypadku wystąpienia szkód, ochronę przed konsekwencjami finansowymi oraz ochronę reputacji.
Jakie mogą być koszty incydentu lub wycieku danych?	Finansowe konsekwencje mogą być dotkliwe: koszty akcji informacyjnej, ekspertów zajmujących się informatyką śledczą, koszty kontroli, roszczenia odszkodowawcze oraz straty związane z zakłóceniem działalności i utratą reputacji.
Dlaczego ważna jest jak najszybsza reakcja?	Szybka reakcja i niwelowanie skutków incydentu cybernetycznego mogą znacznie ograniczyć wyciek danych (poprzez sprawnie udzieloną pomoc ze strony informatyków śledczych). Nowe regulacje prawne nakładają bardzo rygorystyczne obostrzenia. Istotne są sposób i czas, w jakim firma dokona notyfikacji zdarzenia organom administracji oraz zainteresowanym osobom.
Jakie jest ryzyko cyberataku w przypadku MŚP w porównaniu z większymi firmami?	Mniejsze przedsiębiorstwa mogą dysponować gorszymi zabezpieczeniami i nie mieć przygotowanych sprawdzonych procedur działania. Takie firmy często wydają się łatwym celem dla przestępców, którzy mogą chcieć wykorzystać je do przeprowadzenia ataku na większe podmioty.
Czy MŚP zdają sobie sprawę z tego, że ich możliwości w razie wystąpienia szkody są bardziej ograniczone?	Po sforsowaniu ich zabezpieczeń, mniejsze firmy mogą nie mieć dostępu do ekspertów informatyki śledczej, prawników i specjalistów ds. komunikacji. Utrata przychodów, brak możliwości pokrywania kosztów bieżącej działalności oraz utrata reputacji mogą mieć dla nich bardzo poważne konsekwencje.
Większe firmy dysponują większą ilością atrakcyjnych danych. Ryzyko roszczeń ze strony osób trzecich również jest większe.	Duże firmy dysponują większymi ilościami danych, a ewentualny incydent będzie bardziej kosztowny. Ponoszą również większe ryzyko pozwów grupowych o odszkodowania ze strony osób trzecich i akcjonariuszy. Dodatkowo, firmy o znaczeniu strategicznym dla regionu lub państwa są na szczycie listy celów grup cyberprzestępców działających na zlecenie obcych rządów i grup terrorystycznych.
Dużym firmom trudniej jest monitorować tysiące pracowników.	Śledzenie działań pracowników (nieuczciwych lub nieostrożnych), próby odzyskania ukradzionego lub zgubionego sprzętu oraz prowadzenie śledztwa w sprawie wykradzenia informacji zastrzeżonych jest znacznie trudniejsze w przypadku dużych organizacji. Usuwanie skutków naruszenia bezpieczeństwa danych może trwać znacznie dłużej.
Firmy prowadzące działalność za granicą narażone są na dodatkowe komplikacje po skutecznym ataku.	Transgraniczna wymiana danych, nawet wewnątrz przedsiębiorstw, może generować duże koszty związane z usuwaniem skutków szkody. Zagraniczni eksperci, w tym prawnicy, będą musieli współpracować ze sobą, aby zapewnić jak najlepszy rezultat dla klienta.

FIRMY STAJĄ W OBLICZU WIELU ZAGROŻEŃ CYBERNETYCZNYCH

Zaledwie kilka źródeł może stanowić zagrożenie i narażać firmę na nieodwracalne straty.



ARGUMENTY SPRZEDAŻOWE

ARGUMENTY	ROLA UBEZPIECZENIA CYBER GUARD
Nie potrzebujemy tego ubezpieczenia – już takie mamy.	Żadne inne ubezpieczenie nie zapewnia tak kompleksowej ochrony na wypadek skutków zdarzeń cybernetycznych. Inne, takie jak ubezpieczenie ryzyk sprzeniewierzenia, mogą obejmować niektóre elementy, jednak nie zapewniają pełnej ochrony tego typu.
Nie potrzebujemy takiego produktu – nasz system IT jest niezawodny.	Żadna firma nie jest doskonale zabezpieczona przed włamaniem, niezależnie od zabezpieczeń, z jakich korzysta. Bardzo trudno jest monitorować i eliminować wszelkie wewnętrzne i zewnętrzne zagrożenia. Szkodliwe oprogramowanie tworzone jest tak, aby wykorzystywać słabe strony systemu operacyjnego, na które klient nie ma wpływu. Autorzy liczą również na błędy ludzkie, stosując techniki phishingu i vishingu (tzw. phishingu telefonicznego). Dodatkowo, nawet jeśli system klienta byłby niezawodny, najsłabszym ogniwem w cyberprzestrzeni jest człowiek.
Nie potrzebujemy tego ubezpieczenia – nie obejmują nas regulacje prawne dotyczące przetwarzania danych.	Przetwarzając dane osobowe, nawet w niewielkim wolumenie, podlegamy regulacjom w zakresie bezpieczeństwa danych, zarówno tym krajowym jak i międzynarodowym. Odpowiedzialność w świetle przepisów to tylko jeden z wielu kosztów związanych z zagrożeniami cybernetycznymi. Podmioty ponoszą odpowiedzialność wobec klientów za zapewnienie bezpieczeństwa ich danych. Niekorzystny wpływ na reputację w przypadku niepowołanego dostępu do danych może okazać się najbardziej dotkliwą konsekwencją finansową spośród wszystkich kosztów związanych z danym incydentem. Niezależnie od regulacji krajowych, także organizacje branżowe (np. z branży kart płatniczych) mogą nakładać dotkliwe kary finansowe.
Nie potrzebujemy takiego produktu – nasze systemy zabezpieczeń obsługują podmioty zewnętrzne.	Coraz więcej firm przechowuje część danych w chmurze lub powierza ich przechowywanie dostawcom zewnętrznym. Należy zweryfikować standardy bezpieczeństwa po stronie dostawców zewnętrznych, aby upewnić się, że są odpowiednie. Biorąc pod uwagę charakter działalności i ilość przechowywanych danych, takie podmioty stają się atrakcyjnym celem przestępców. Umowy podpisywane z zewnętrznymi dostawcami rozwiązań w zakresie bezpieczeństwa często ograniczają odpowiedzialność w przypadku włamania, więc firma sama musi ponieść koszty związane z eliminacją skutków oraz koszty obrony.
Nie działamy w „atrakcyjnej" dla przestępców branży.	Cyberprzestępcy, pracownicy lub konkurencja mogą być zainteresowani przetwarzanymi przez firmę danymi. Przestępcy często wykorzystują pozornie „nieatrakcyjne" firmy, aby uzyskać dostęp do większych, bardziej atrakcyjnych podmiotów. Jeżeli okaże się, że państwa klient ponosi winę za włamanie do sytemu informatycznego jego kontrahenta (np. wprowadzenie poprzez systemy informatyczne klienta złośliwego oprogramowania do systemu informatycznego kontrahenta), czy będzie on w stanie ponieść odpowiedzialność z tym związaną?
Ubezpieczenie jest za drogie.	Składki są niewielkie w porównaniu z potencjalnymi konsekwencjami finansowymi zdarzenia. Siedmiocyfrowe straty nie są rzadkością w przypadku utraty zaufania klientów. Ubezpieczenie ryzyk cybernetycznych to przystępna cenowo i przewidywalna inwestycja w ochronę firmy na wypadek niepowołanego dostępu do danych.
Nie potrzebujemy takiego produktu – nasza infrastruktura jest niezawodna.	Zgubione lub skradzione laptopy i inny sprzęt komputerowy to bardzo częste przyczyny naruszeń bezpieczeństwa. Jeżeli firma nie zapewnia „fizycznego" bezpieczeństwa swojej infrastruktury, istnieje duże zagrożenie dla bezpieczeństwa danych. Warto również pamiętać, że wielokrotnie to lekkomyślność pracowników lub niewłaściwe podejście człowieka do zabezpieczeń oraz brak przeszkolenia wpływają na zawodność zabezpieczeń firmy.
Firma jest mała – nic nam nie grozi.	Duże podmioty stale wzmacniają zabezpieczenia swojej firmowej infrastruktury, dlatego przestępcy zaczęli rozglądać się za mniejszymi, łatwiejszymi celami. Większość włamań ma miejsce w firmach zatrudniających do 100 pracowników. Zatem mniejsze firmy powinny dysponować środkami pozwalającymi skutecznie się zabezpieczyć, zapobiec szkodzie i usunąć jej skutki.
Nigdy nie miałem z niczym takim do czynienia, więc nie potrzebuję tego ubezpieczenia.	Przedsiębiorstwa są obecnie znacznie bardziej narażone na zagrożenia związane z bezpieczeństwem i poufnością danych. Powstające przepisy (RODO) zaostrzają obowiązujące normy, co może spowodować, że konsekwencje finansowe i wpływ na działalność firm, które padły ofiarą włamania lub które się do niego przyczyniły mogą być bardziej uciążliwe. Kary administracyjne mogą sięgać 20 mln euro, jednak oprócz kar należy pamiętać o rygorystycznych wymogach notyfikacyjnych (72 godziny).

PRZYKŁADY ROSZCZEŃ

OPIS	OCHRONA W RAMACH CYBER GUARD
NIEUCZCIWY PRACOWNIK **Pracownik dużej agencji gromadzącej dane o historii kredytowej konsumentów wykrada dane osobowe milionów klientów.**	▪ Koszty ekspertyz mających na celu ustalenie, które dane zostały wykradzione i których osób dotyczyły. ▪ Koszty akcji informacyjnej wśród milionów osób, których dane zostały wykradzione. ▪ Koszty radcy prawnego, który przygotuje firmę do wzięcia udziału w dochodzeniu dotyczącym incydentu. ▪ Koszty reprezentacji i obrony firmy w wytoczonym procesie. ▪ Koszty zasądzonych odszkodowań.
UTRATA DANYCH PRZEZ FIRMĘ ZEWNĘTRZNĄ **Firmowy serwer poczty elektronicznej wraz z dyskiem twardym został skradziony firmie zewnętrznej, której zlecono przechowywanie danych.**	▪ Koszty ekspertyz w celu ustalenia, jakie dane zostały skradzione i których osób dotyczyły. ▪ Koszty akcji informacyjnej wśród osób, których dane zostały wykradzione. ▪ Koszty radcy prawnego, który przygotuje firmę do wzięcia udziału w dochodzeniu dotyczącym incydentu. ▪ Koszty porad w zakresie usług PR, zapewniających firmie wsparcie i poprowadzenie komunikacji zewnętrznej dotyczącej incydentu.
WŁAMANIE – HOTEL **Hakerzy uzyskują dostęp do systemów komputerowych 26 hoteli.**	▪ Koszty ekspertyz w celu ustalenia, jakie dane zostały skradzione i których osób dotyczyły (prawie pół miliona danych o kartach kredytowych i ich właścicielach). ▪ Koszty akcji informacyjnej wśród osób, których dane zostały wykradzione. ▪ Koszty radcy prawnego, który przygotuje firmę do wzięcia udziału w dochodzeniu dotyczącym incydentu. ▪ Koszty porad w zakresie PR, aby zminimalizować niekorzystny wpływ na reputację.
WŁAMANIE – KARTY **Następuje włamanie do systemu podmiotu przetwarzającego operacje na kartach – następuje utrata danych dotyczących kart kredytowych.**	▪ Koszty ekspertyz w celu ustalenia, jakie dane zostały skradzione i których osób dotyczyły. ▪ Koszty akcji informacyjnej wśród milionów osób, których dane zostały wykradzione. ▪ Koszty porad w zakresie PR, aby zminimalizować niekorzystny wpływ włamania na reputację firmy. ▪ Koszty radcy prawnego, który przygotuje firmę do wzięcia udziału w dochodzeniu dotyczącym incydentu. ▪ Koszty reprezentacji podczas dochodzenia przed organizacjami branżowymi rynku kart płatniczych. ▪ Koszty reprezentacji i obrony w trakcie procesu wytoczonego przeciwko firmie.

Inne scenariusze szkód:

SYSTEM SPRZEDAŻY (POS)
System sprzedaży w supermarkecie został zaatakowany przez szkodliwe oprogramowanie pochodzące z zewnątrz, co spowodowało zerwanie komunikacji pomiędzy kasami a urządzeniem monitorującym stany magazynowe. Na skutek ataku supermarketowi skończyły się zapasy i zamknięto go do czasu naprawienia systemu i uzupełnienia towarów.

REJESTRACJA SEKWENCJI NACISKANYCH KLAWISZY
Włamano się do systemu sprzedażowego ponad 200 placówek handlowych (w tym 150 placówek restauracji sieciowej) i wprowadzono do niego tzw. keyloggery, czyli oprogramowanie zapisujące sekwencje naciskanych klawiszy w systemie oraz dane kart przeciąganych w terminalach.

TAŚMY ZAWIERAJĄCE KOPIE ZAPASOWE
Brytyjski organ nadzoru nałożył na międzynarodowe towarzystwo ubezpieczeniowe karę w wysokości wielu milionów funtów po tym, jak zgubiono taśmę zawierającą kopię zapasową danych osobowych ponad 46 tys. właścicieli polis.

DŁUGOTRWAŁE DZIAŁANIA PRZESTĘPCZE
Przez 4 lata pewna grupa przestępcza wykradła poufne informacje z wielu największych firm z sektora paliwowego i energetycznego. Dzięki wykorzystaniu technik haszowania kluczy wyprowadzono dane osobowe i dane merytoryczne dotyczące wydobycia ropy i umów pomiędzy współpracującymi firmami, których systemy zarażono złośliwym oprogramowaniem.

PODSUMOWANIE ZAKRESU UBEZPIECZENIA

KOSZTY FINANSOWE

Koszty finansowe w przypadku odpowiedzialności firmy wobec osób trzecich	▪ Koszty obrony i odszkodowań, w przypadku gdy firma (lub podmiot, któremu powierza wykonywanie pewnych czynności) spowoduje naruszenie bezpieczeństwa danych osobowych lub informacji handlowych. ▪ Koszty obrony i odszkodowań, w przypadku gdy firma spowoduje wprowadzenie wirusa do danych osób trzecich lub systemu informatycznego osób trzecich. ▪ Koszty obrony i odszkodowań, w przypadku gdy firmie ukradziony zostanie kod dostępu do sieci w sposób inny niż elektroniczny. ▪ Koszty obrony i odszkodowań, w przypadku gdy firmie ukradziony zostanie sprzęt komputerowy, na którym przechowywane są dane osobowe. ▪ Koszty obrony i odszkodowań, w przypadku gdy pracownik firmy spowoduje ujawnienie danych osób trzecich.
Koszty finansowe związane z wymogami prawnymi dotyczącymi ochrony danych	▪ Koszty porad prawnych i reprezentacji w postępowaniach administracyjnych prowadzonych przez organ nadzoru ds. ochrony danych. ▪ Kary administracyjne za naruszenie danych nakładane przez organ nadzoru ds. ochrony danych. ▪ Koszty powiadomienia osób, których dane wyciekły (lub powiadomienia o tym zdarzeniu regulatora) o tym, że do ich danych uzyskano niepowołany dostęp.

USŁUGI KONSULTINGOWE

Eksperckie usługi konsultingowe w zakresie IT na rzecz firmy w czasie incydentu oraz po nim	▪ Koszty usług świadczonych przez specjalistów w zakresie informatyki śledczej zapewniające wsparcie, gdy klient podejrzewa włamanie. ▪ Koszty specjalistów w zakresie informatyki śledczej po incydencie naruszenia bezpieczeństwa danych ubezpieczonego, mające na celu wydanie rekomendacji w zakresie ograniczenia ryzyka wystąpienia naruszenia bezpieczeństwa danych w przyszłości. ▪ Koszty usług eksperckich w celu ustalenia, czy dane elektroniczne można odtworzyć, ponownie zgromadzić lub stworzyć od nowa. ▪ Koszty usług eksperckich w zakresie odzyskania danych.
Wsparcie merytoryczne w celu ochrony i odbudowy reputacji firmy po włamaniu	▪ Koszty konsultacji eksperckich, mających na celu zapobieżenie ewentualnym niekorzystnym wpływom głośnych incydentów lub zminimalizowanie ich skutków. ▪ Koszty konsultacji eksperckich, mających na celu zminimalizowanie utraty reputacji przez pracownika firmy (np. członka zarządu, któremu powierzono ochronę danych).

OPCJONALNE ZAKRESY UBEZPIECZENIA

Zakłócenia w działaniu sieci	▪ Pokrycie kosztów utraty zysku spowodowanego zakłóceniem działania sieci ubezpieczonego w następstwie naruszenia bezpieczeństwa danych.
Próba szantażu	▪ Pokrycie kosztów niezależnych doradców w celu ustalenia okoliczności szantażu, jak również kwoty okupu na rzecz osoby trzeciej grożącej ujawnieniem poufnych informacji bezprawnie uzyskanych z baz danych ubezpieczonego.
Działalność multimedialna	▪ Pokrycie szkód i kosztów obrony prawnej poniesionych wskutek naruszenia praw ochrony własności intelektualnej osoby trzeciej w związku z treściami przekazywanymi za pośrednictwem mediów cyfrowych.

Pełne brzmienie zakresu i warunków znajduje się w ogólnych warunkach ubezpieczenia CYBER GUARD.

UBEZPIECZENIA INSPIROWANE **LUDŹMI**

COLONNADE INSURANCE SOCIETE ANONYME ODDZIAŁ W POLSCE

ul. Marszałkowska 111
00-102 Warszawa
Polska

tel. +48 22 528 51 00
fax +48 22 528 52 52

e-mail: info@colonnade.pl
www.colonnade.pl

COLONNADE
A FAIRFAX COMPANY