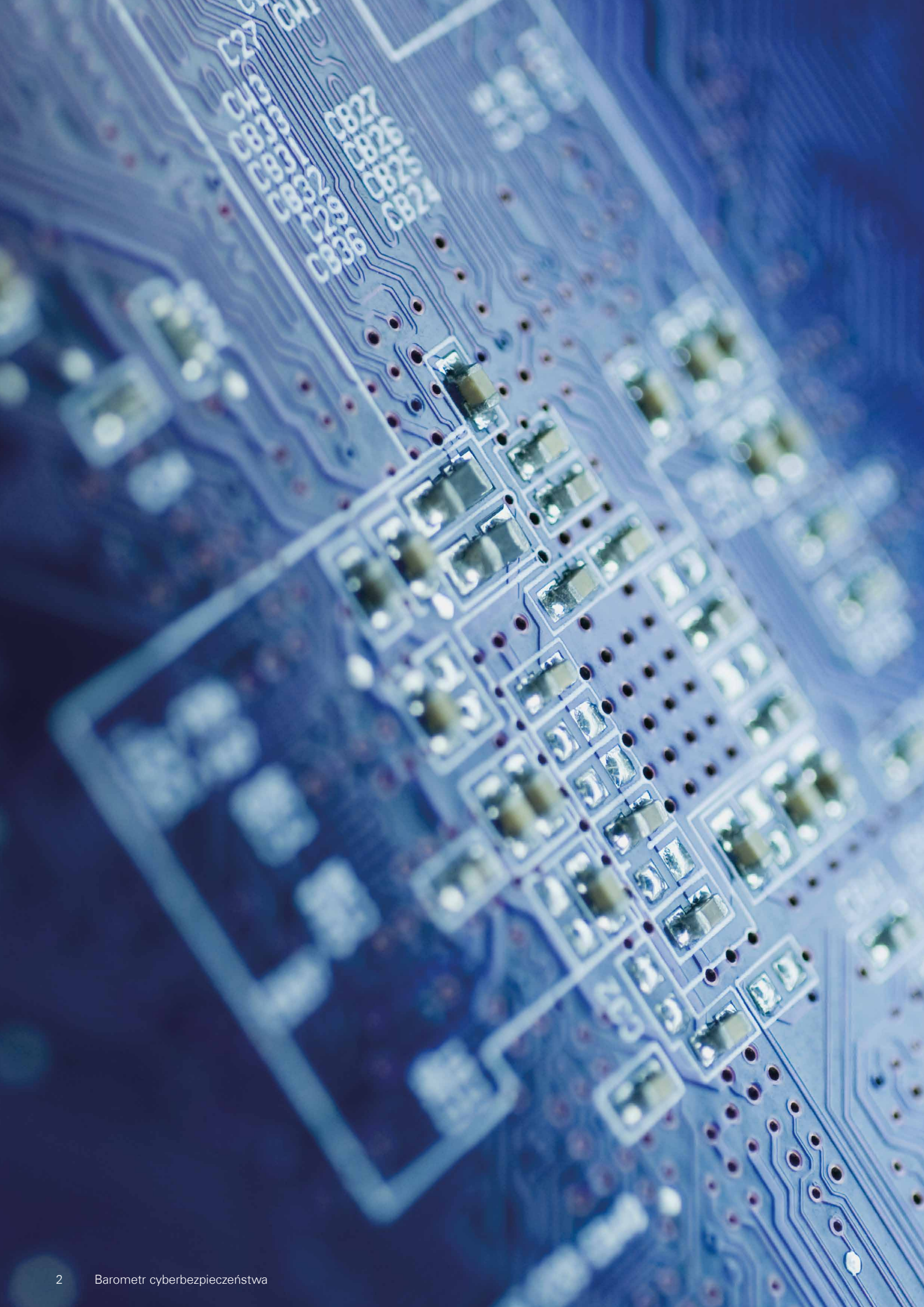
KPMG

Barometr cyberbezpieczeństwa

Cyberatak zjawiskiem powszechnym

Styczeń 2018

KPMG.pl



Szanowni Państwo

Zachęcamy do zapoznania się z wynikami badania KPMG „Barometr cyberbezpieczeństwa" diagnozującego bieżące trendy i podejście polskich przedsiębiorstw w zakresie ochrony przed cyberprzestępczością. W badaniu wzięło udział ponad 100 małych, średnich i dużych polskich firm, reprezentowanych przez osoby odpowiedzialne za zapewnienie bezpieczeństwa informacji.

Patrząc na skalę odnotowanych w Polsce w 2017 roku cyberataków, obejmujących m.in. ataki ukierunkowane na sektor bankowy, czy światowej skali kampanie ransomware, nie dziwi fakt, że niemal każda polska firma została dotknięta przez cyberprzestępczość. Wyniki raportu jednoznacznie wskazują, że firmy odnotowały wzrost skali cyberzagrożeń.

Polskie przedsiębiorstwa najbardziej obawiają się zorganizowanej cyberprzestępczości. W szczególności trudnych do zidentyfikowania i odparcia ataków ukierunkowanych, cyberprzestępstw realizowanych za pośrednictwem złośliwego oprogramowania oraz wspieranych przez socjotechnikę. Własny pracownik, który historycznie stanowił dla firm najczęstsze źródło naruszeń bezpieczeństwa, zszedł na drugi plan.

Ciekawym wynikiem badania jest wysoki optymizm polskich przedsiębiorstw w kwestii oceny dojrzałości wdrożonych zabezpieczeń. Z perspektywy doświadczeń KPMG z realizowanych audytów bezpieczeństwa, wydaje się, że tak wysoka samoocena, może niestety po części wynikać z wciąż niedostatecznej świadomości polskich firm w zakresie skali i złożoności dzisiejszych cyberzagrożeń. Pozytywnym natomiast sygnałem jest fakt, że firmy inwestują w mechanizmy bezpieczeństwa pozwalające na wczesną identyfikację i reakcję na cyberatak, co jest zgodne z globalnym podejściem w zakresie cyberbezpieczeństwa, zakładającym, że cyberatak jest dziś zjawiskiem nieuchronnym i należy się na niego przygotować.

Biorąc pod uwagę szczególny okres, w którym przeprowadziliśmy badanie, zapytaliśmy polskie firmy o status przygotowań do zgodności z nowymi regulacjami w zakresie ochrony danych osobowych (RODO). Jedynie co czwarta firma deklaruje zgodność, natomiast aż 38% przedsiębiorstw nie rozpoczęło jeszcze żadnych działań w tym zakresie. Biorąc pod uwagę liczbę zmian, które muszą zostać wdrożone zgodnie z nowymi przepisami, istnieje duże ryzyko, że większość przedsiębiorstw w Polsce nie dopełni wszystkich wymogów formalnych do 25 maja 2018 roku, narażając się tym samym na istotne konsekwencje finansowe.

Pozostaje nam życzyć Państwu przyjemnej lektury oraz wielu przemyśleń i inspiracji, które przyczynią się do wzrostu bezpieczeństwa w Państwa organizacjach.

Michał Kurek
Partner KPMG,
Szef zespołu ds.
cyberbezpieczeństwa

Krzysztof Radziwon
Partner KPMG,
Szef zespołu ds.
zarządzania ryzykiem

Najważniejsze wnioski

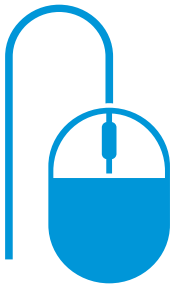
Cyberataki są zjawiskiem powszechnym

wśród firm działających w Polsce. 82% przedsiębiorstw odnotowało przynajmniej jeden cyberincydent w 2017 roku.

37% firm odnotowało

wzrost liczby cyberataków

w przeciągu ostatniego roku (podczas gdy spadek stwierdziło tylko 5%).

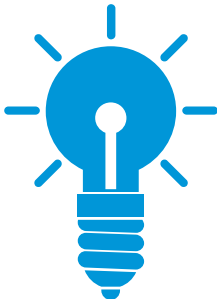


Zorganizowane grupy cyberprzestępcze

(dla 62% respondentów) i pojedynczy hakerzy (dla 61% firm) są najczęstszymi źródłami ataków.
Dopiero na trzecim miejscu znalazł się niezadowolony lub podkupiony pracownik, który historycznie był najbardziej istotnym źródłem.

Najgroźniejsze cyberzagrożenia

dla firm to: malware (APT, wycieki danych, ransomware), czynnik ludzki (kradzież danych przez pracowników, phishing) i ataki na aplikacje.



Większość firm optymistycznie ocenia dojrzałość stosowanych zabezpieczeń, czego powodem może być m.in.

niedoszacowanie ryzyka.

Blisko połowa firm wykorzystuje

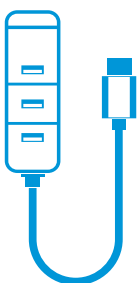
outsourcing usług bezpieczeństwa

w zakresie wsparcia w reakcji na występienie cyberataku.

Dla 49% firm zatrudnienie i utrzymanie wykwalifikowanych pracowników jest

największym wyzwaniem

w zakresie uzyskania oczekiwanego poziomu zabezpieczeń, istotniejszym nawet niż niewystarczający budżet (47% respondentów).



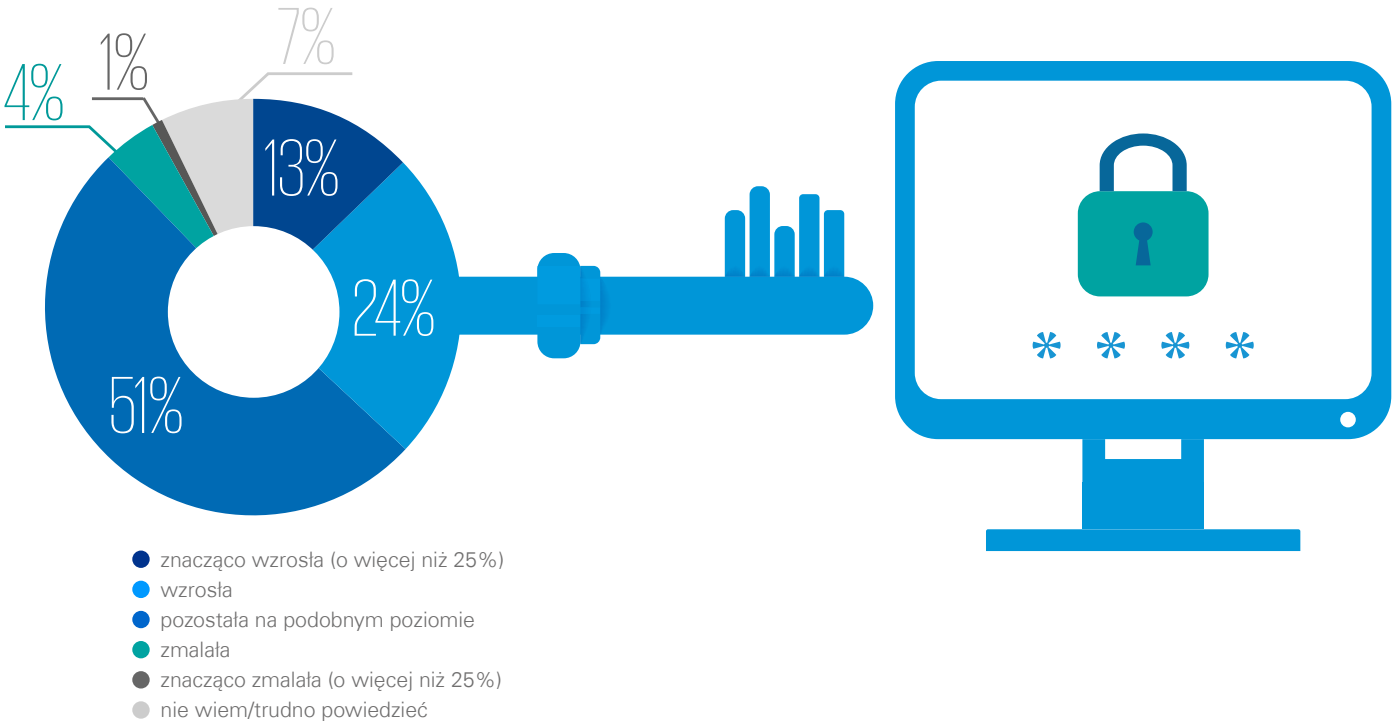
Łącznie aż 38% firm nie realizuje żadnych działań lub nie rozpoczęło analizy luk weryfikującej

zgodność z wymogami RODO.

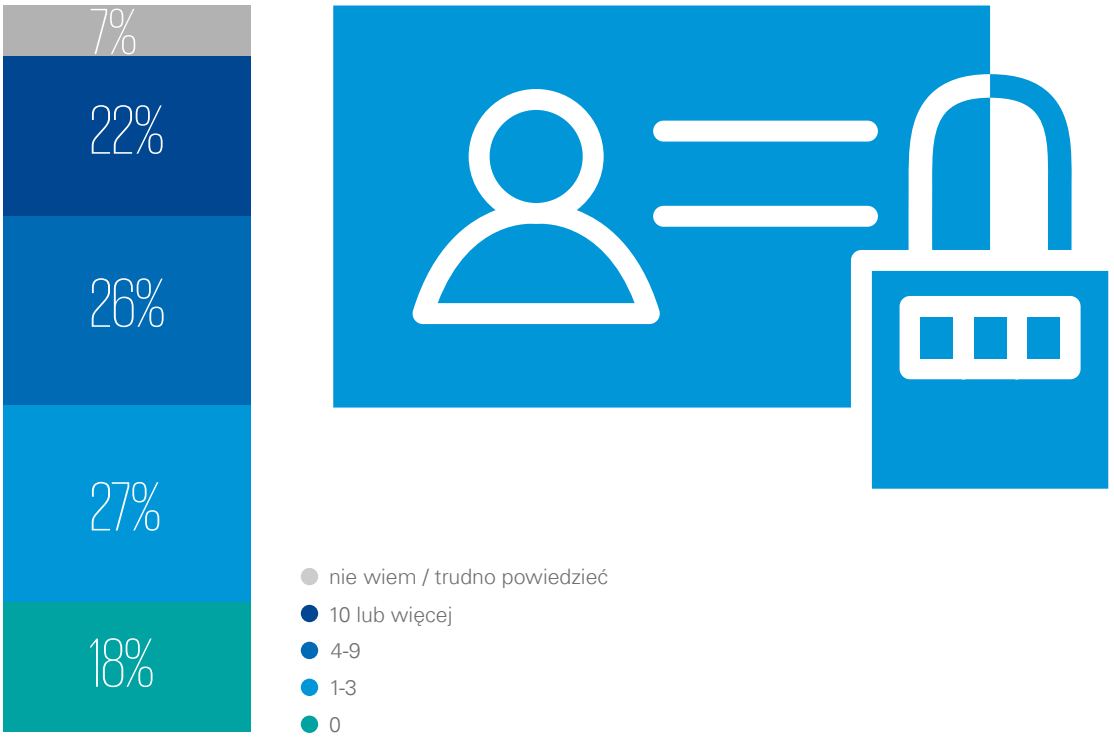
Skala cyberataków na firmy w Polsce

37% firm w Polsce zadeklarowało wzrost lub znaczący wzrost liczby cyberataków, podczas gdy tylko 5% odnotowało spadek. Jedynie 18% firm nie odnotowało w 2017 roku żadnego cyberataku.

W 2017 roku liczba zaobserwowanych w organizacji prób cyberataków, w porównaniu z poprzednim rokiem:



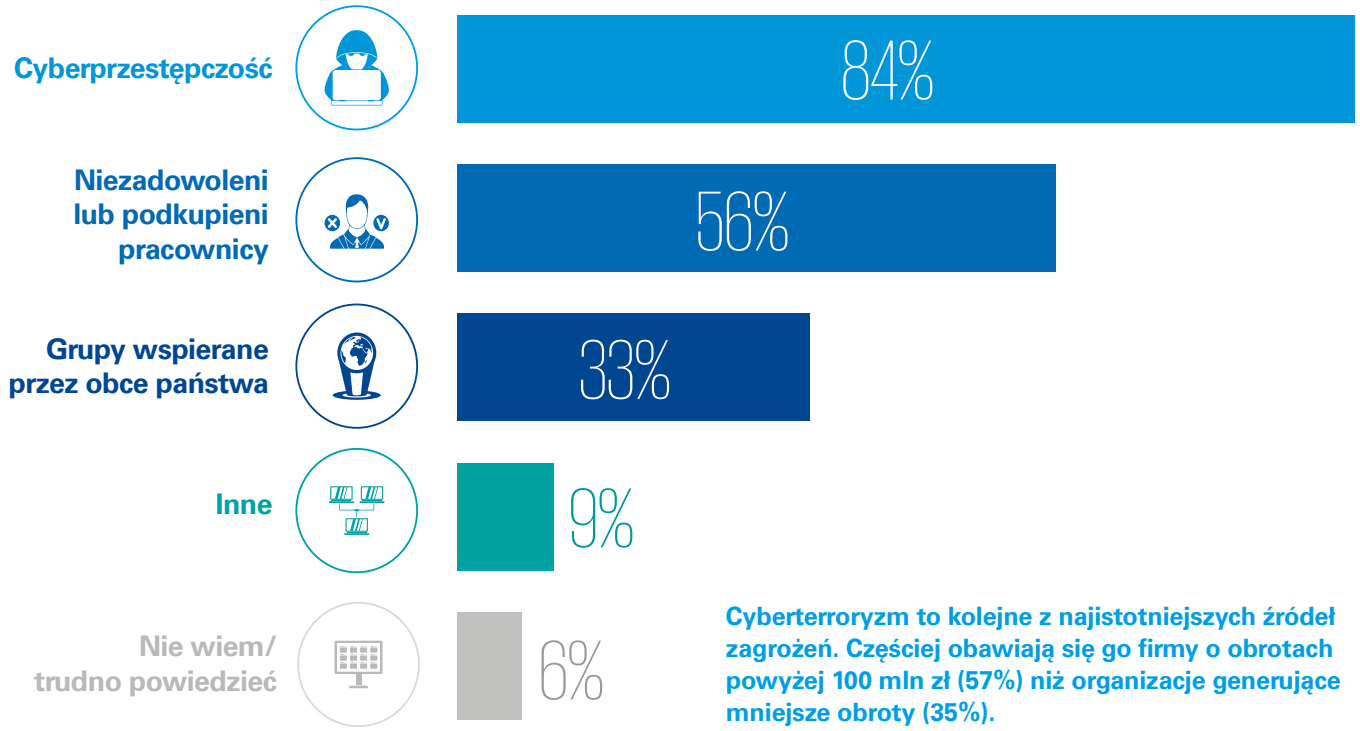
Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa w 2017 roku wyniosła:



Źródła cyberzagrożeń

Szeroko rozumiana cyberprzestępczość stanowi najistotniejsze źródło zagrożeń dla największego odsetka firm w Polsce. Niezadowolony lub podkupiony pracownik, który przed kilkoma laty był problemem nr 1, schodzi na drugi plan.

Które z poniższych grup lub osób stanowią realne zagrożenie dla firm?

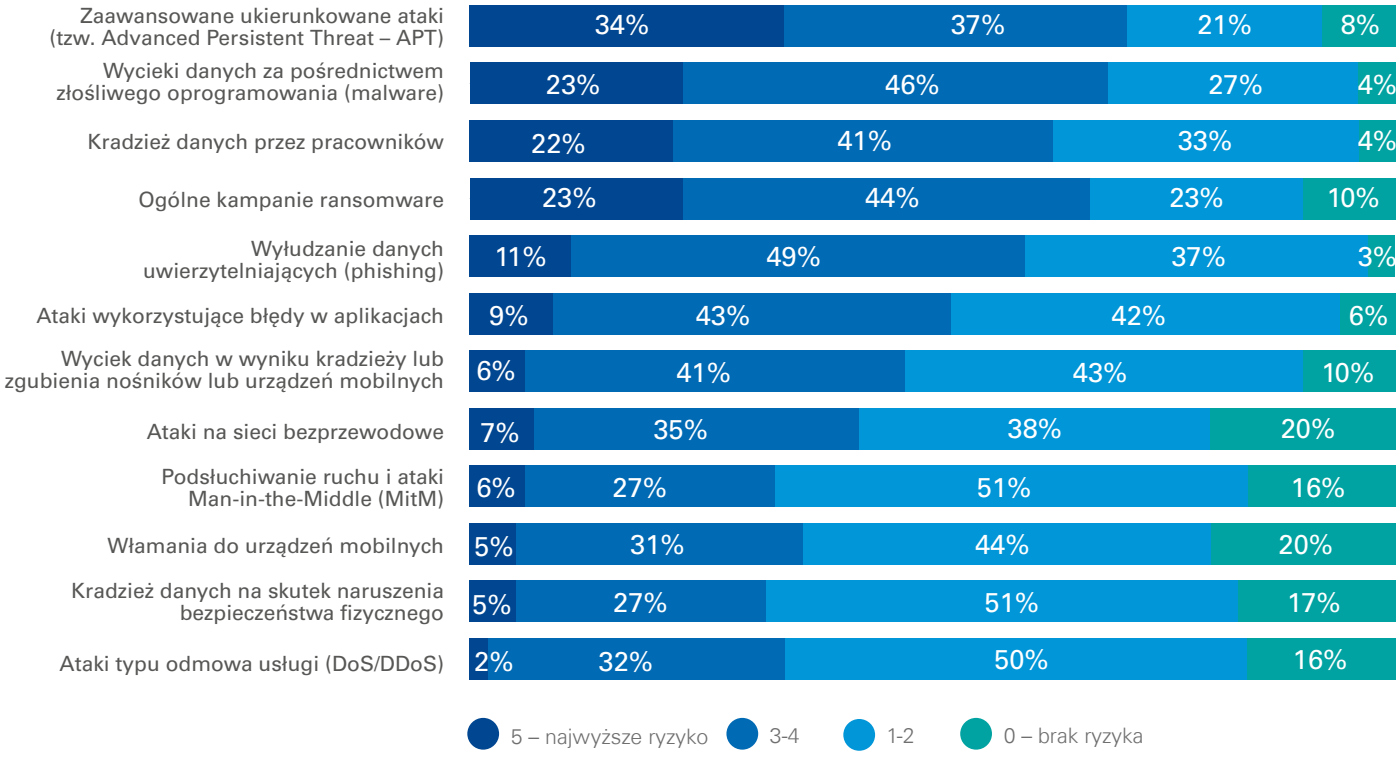


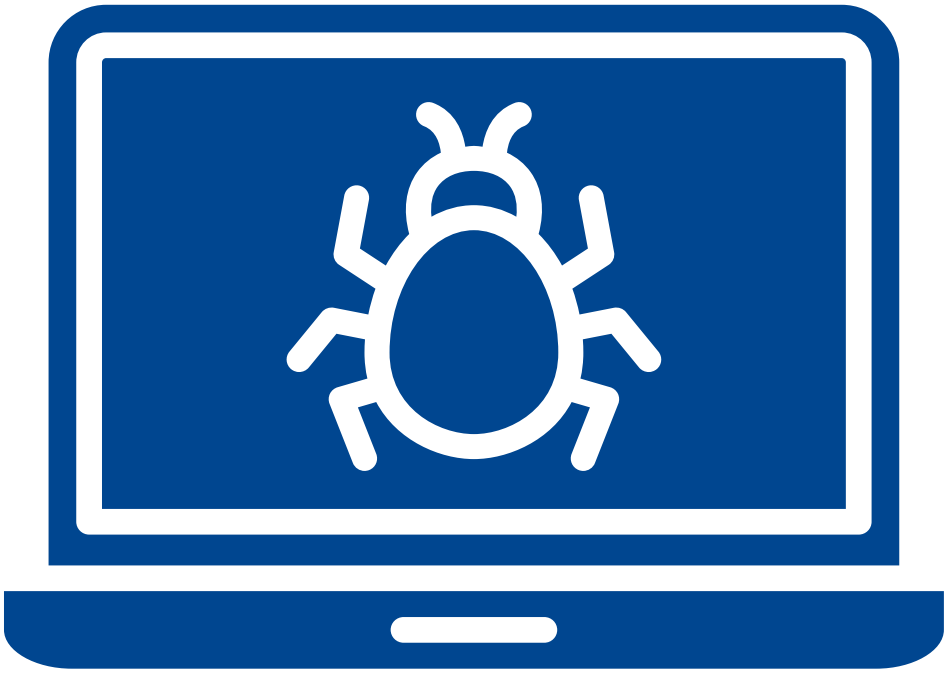
Cyberterroryzm to kolejne z najistotniejszych źródeł zagrożeń. Częściej obawiają się go firmy o obrotach powyżej 100 mln zł (57%) niż organizacje generujące mniejsze obroty (35%).

Największe cyberzagrożenia

Ankietowane firmy najbardziej obawiają się złośliwego oprogramowania (stosowanego do ataków ukierunkowanych APT, kradzieży danych czy wymuszania okupu), słabości czynnika ludzkiego (phishing, kradzież danych przez pracowników) oraz ataków na aplikacje. Najmniejsze obawy respondentów budzą ataki typu odmowa usługi (DoS/DDoS) czy kradzież danych na skutek naruszenia bezpieczeństwa fizycznego. Należy jednak zachować ostrożność, ponieważ mniejsze obawy w tym zakresie mogą oznaczać niedoszacowanie ryzyka przez respondentów.

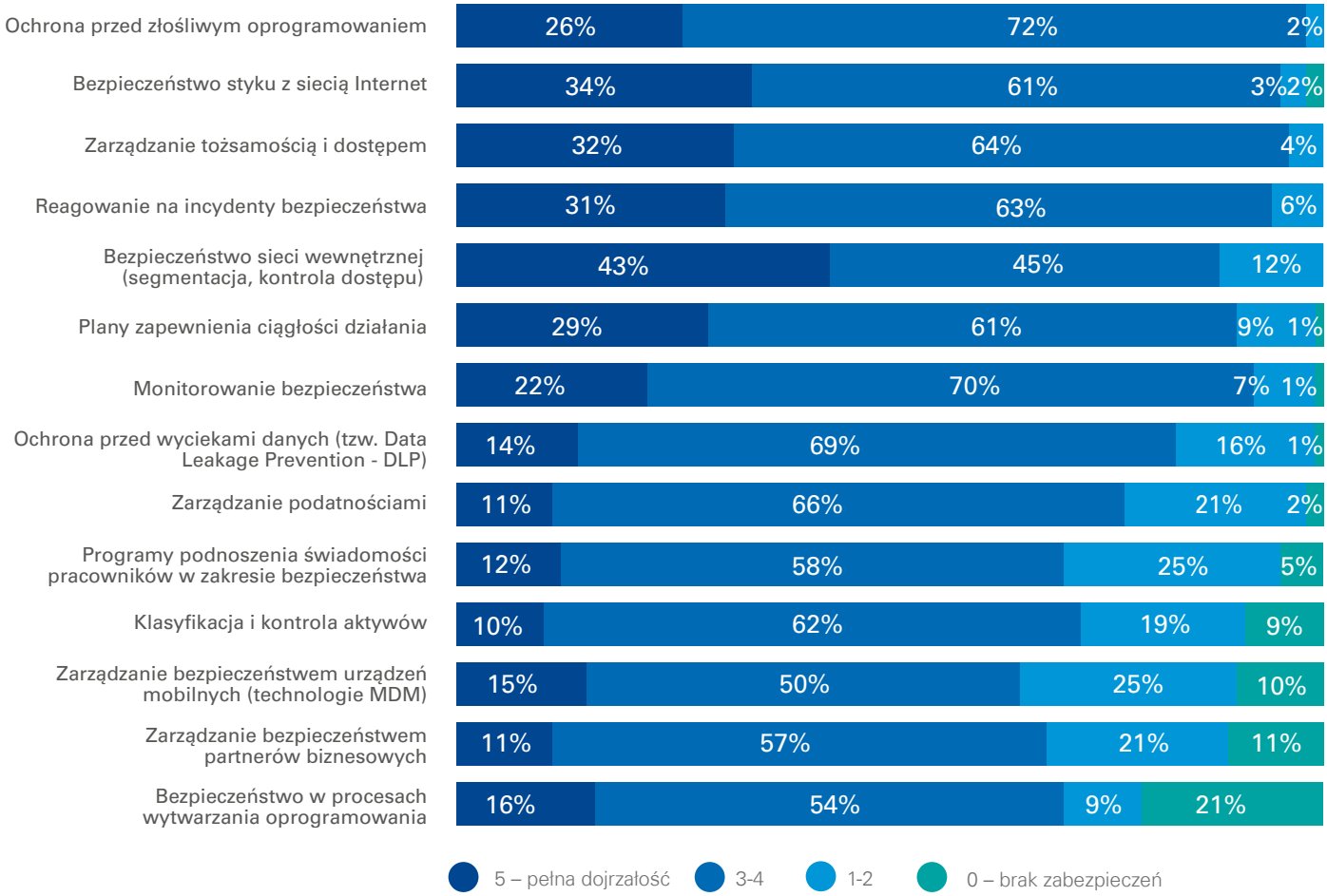
Które z poniższych cyberzagrożeń stanowią największe ryzyko dla organizacji?





Dojrzałość obszarów zabezpieczeń

Jak firmy oceniają dojrzałość poszczególnych obszarów zabezpieczeń w swoich organizacjach?



1

Analizując ocenę dojrzałości i skłonność do inwestycji polskich firm w zabezpieczenia alarmujące jest podejście do włączania bezpieczeństwa w procesy wytwarzania aplikacji. Jest to obszar najmniej dojrzały i wygląda na to, że sytuacja nie ulegnie poprawie. Czy dziurawe aplikacje nadal będą zjawiskiem powszechnym?

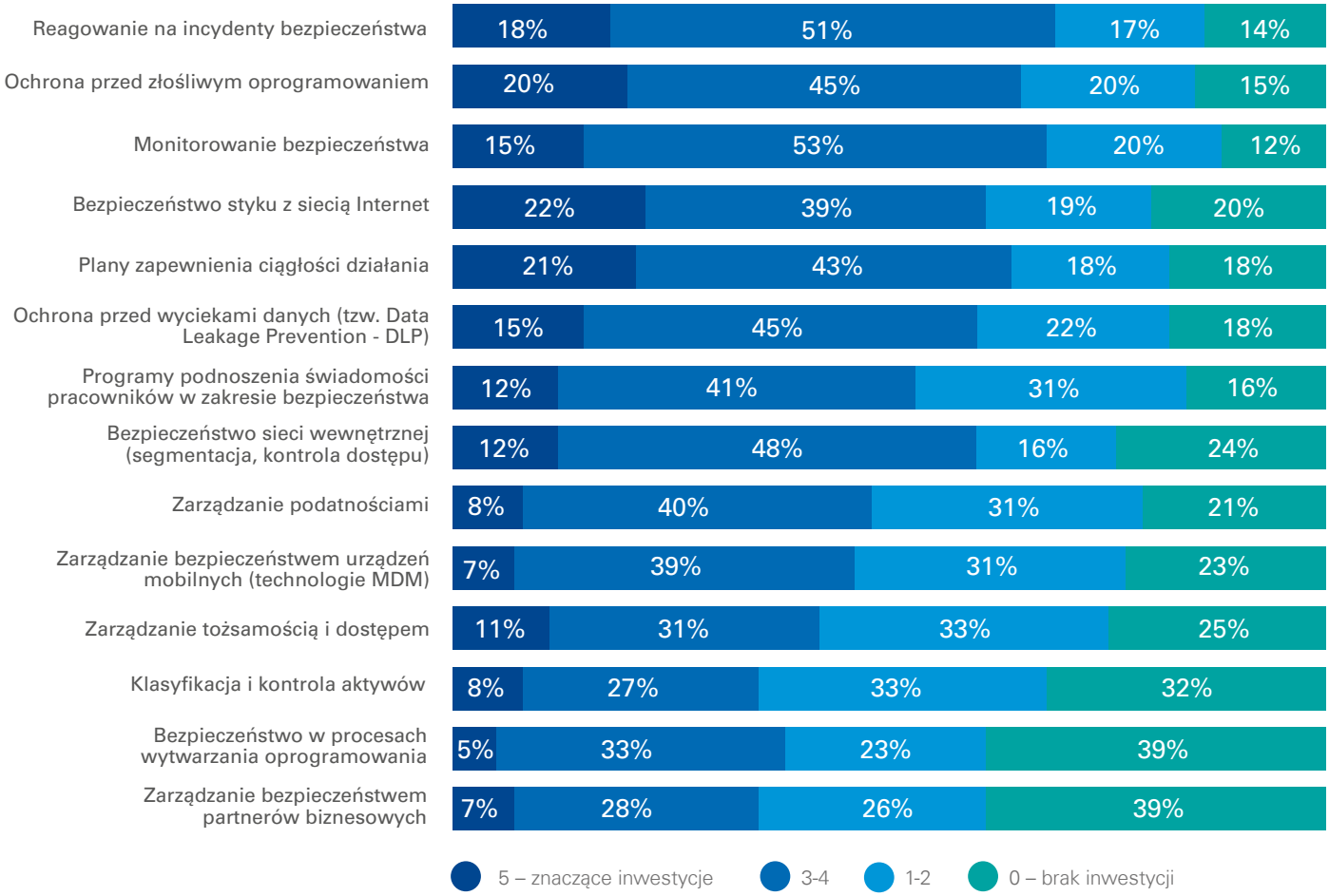
2

Niepokoi także niska skłonność do inwestycji w zarządzanie bezpieczeństwem u partnerów biznesowych. Obszar ten staje się szczególnie istotny w świetle nowych regulacji w zakresie ochrony danych osobowych.

3

Trzecim z niewystarczająco rozwijanych obszarów zabezpieczeń jest klasyfikacja i kontrola aktywów, który w obliczu niewystarczających zasobów staje się jednym z podstawowych elementów skutecznego systemu zarządzania bezpieczeństwem.

Planowane inwestycje w obszary zabezpieczeń

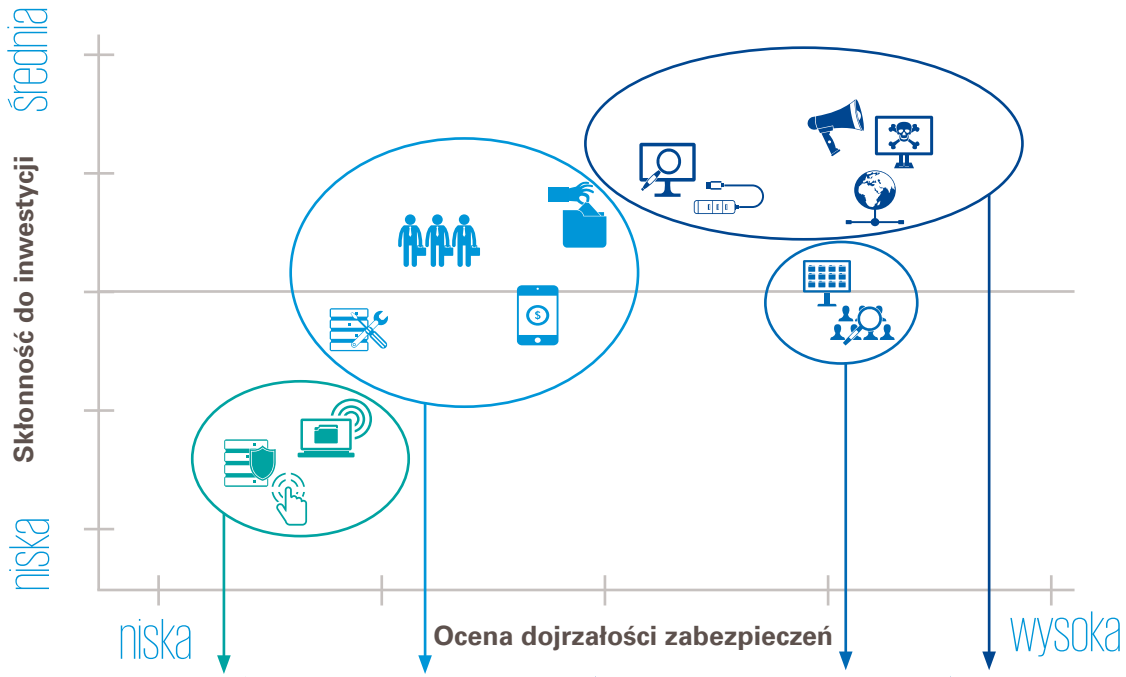


4 Warto zwrócić również uwagę na podejście do podnoszenia świadomości użytkowników w zakresie cyberbezpieczeństwa oraz do ochrony urządzeń mobilnych, które w obliczu obserwowanych zmian w sposobie działania cyberprzestępców będą nabierały znaczenia.

5 Niepokoi również relatywnie niska dojrzałość obszaru zarządzania podatnościami, który jest krytycznym elementem systemu zabezpieczeń.

6 Pozytywnym natomiast sygnałem jest fakt, że firmy inwestują w monitorowanie bezpieczeństwa i reagowanie na cyberataki, co jest zgodne z globalnym podejściem w zakresie cyberbezpieczeństwa, zakładającym, że cyberatak jest zjawiskiem nieuchronnym i należy się na niego przygotować.

Obszary zabezpieczeń – dojrzałość a planowane inwestycje

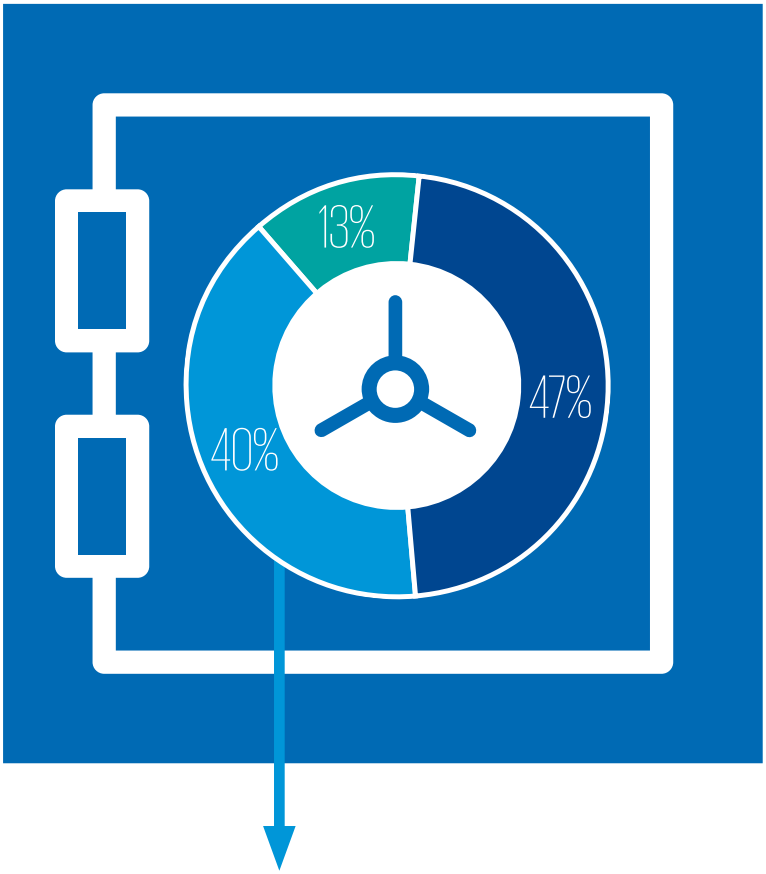


Obszary mniej dojrzałe, zagrożone ryzykiem niedofinansowania	Obszary mniej dojrzałe, niskobudżetowe	Obszary dojrzałe, niskobudżetowe	Obszary dojrzałe, o średnim budżecie
Klasyfikacja i kontrola aktywów	Ochrona przed wyciekami danych	Bezpieczeństwo sieci wewnętrznej	Reagowanie na incydenty bezpieczeństwa
Zarządzanie bezpieczeństwem partnerów biznesowych	Zarządzanie podatnościami	Zarządzanie tożsamością i dostępem	Ochrona przed złośliwym oprogramowaniem
Bezpieczeństwo w procesach wytwarzania oprogramowania	Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa		Monitorowanie bezpieczeństwa
	Zarządzanie bezpieczeństwem urządzeń mobilnych		Plany zapewnienia ciągłości działania
			Bezpieczeństwo styku z siecią Internet

Odpowiedzialność za obszar bezpieczeństwa informacji

Wiele jest do zrobienia w kwestii organizacji bezpieczeństwa. Jedynie co dziesiąta firma posiada dedykowaną do tego jednostkę organizacyjną.

Do kogo w organizacji przypisana jest odpowiedzialność za obszar bezpieczeństwa informacji?



- Dyrektor IT (CIO) lub dedykowany pracownik w strukturach IT
- Inne stanowisko
- Brak formalnego przypisania odpowiedzialności

Prezes zarządu (CEO) — 11%

Niezależna dedykowana funkcja (CSO/CISO) — 11%

Inne stanowisko w organizacji niż powyższe — 11%

Odpowiedzialność przypisana w strukturach globalnych poza Polską — 7%

Co blokuje firmy w budowaniu cyberbezpieczeństwa?

Brak wykwalifikowanych pracowników okazał się najważniejszym problemem dla firm przy budowaniu cyberbezpieczeństwa. Istotniejszym nawet od niewystarczających budżetów, które są zwykle czołowym wyzwaniem. Firmy skarżą się również na brak dobrze zdefiniowanych mierników, co wskazuje na rosnącą potrzebę monitorowania poziomu faktycznie uzyskiwanego bezpieczeństwa.

Jakie są główne ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w firmach?

49%
Trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników

47%
Brak wystarczających budżetów

46%
Brak dobrze zdefiniowanych mierników

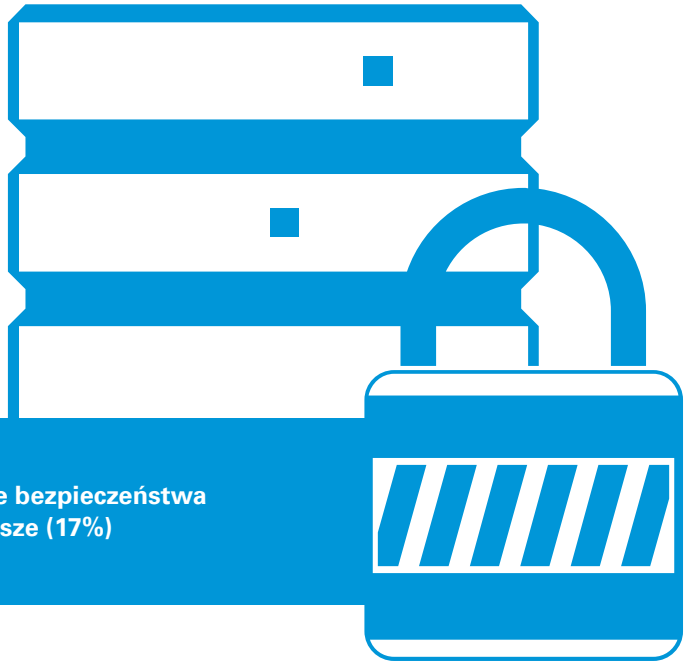
26%
Brak właściwego przypisania odpowiedzialności w zakresie bezpieczeństwa

25%
Brak zaangażowania biznesu

17%
Brak wsparcia najwyższego kierownictwa

15%
Inne

14%
Nie wiem/trudno powiedzieć



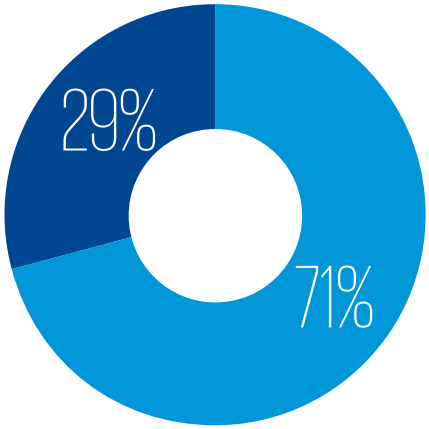
Brak właściwie przypisanej odpowiedzialności w zakresie bezpieczeństwa był częściej wskazywany przez małe firmy (55%) niż większe (17%)

Outsourcing cyberbezpieczeństwa sposobem na problemy kadrowe

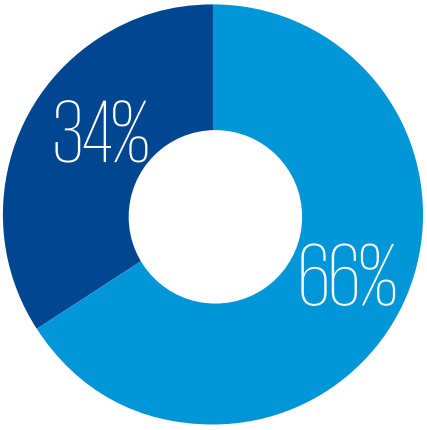
71% badanych firm korzysta z outsourcingu w zakresie usług bezpieczeństwa. Z usług zewnętrznego dostawcy częściej korzystają firmy z kapitałem zagranicznym (86%) niż organizacje z polskim kapitałem (66%).

Które z poniższych funkcji lub procesów bezpieczeństwa są realizowane przez dostawców (outsourcing)?

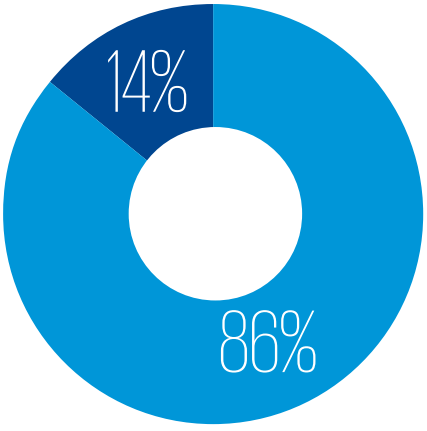
Korzystanie z outsourcingu



przez firmy z polskim kapitałem



przez firmy kapitałem zagranicznym

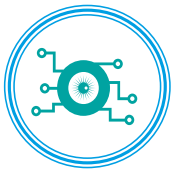


tak
nie

Funkcje / procesy bezpieczeństwa realizowane przez dostawców

49%
Wsparcie w reakcji na cyberataki

38%
Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa



38%
Testy podatności infrastruktury

37%
Monitorowanie bezpieczeństwa

33%
Analiza złośliwego oprogramowania

31%
Testy penetracyjne aplikacji

30%
Przeglądy kodu źródłowego

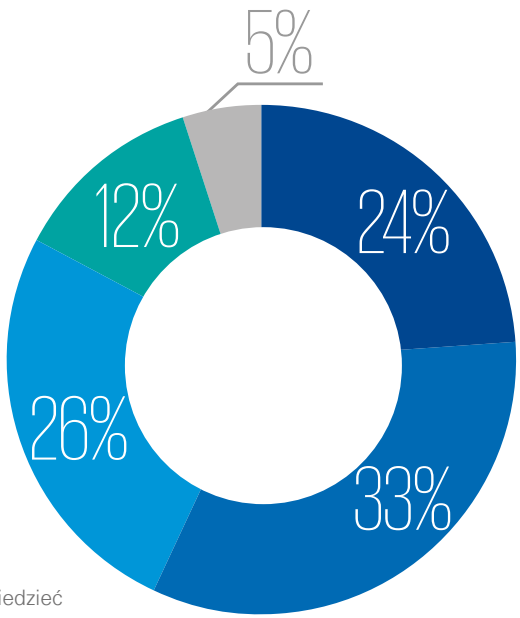
29%
Żadne z powyższych

Status przygotowań do zapewnienia zgodności z wymogami RODO

Dla znaczącej większości polskich firm (76%) istnieje realne ryzyko braku pełnej zgodności z RODO przed dniem jego obowiązywania.

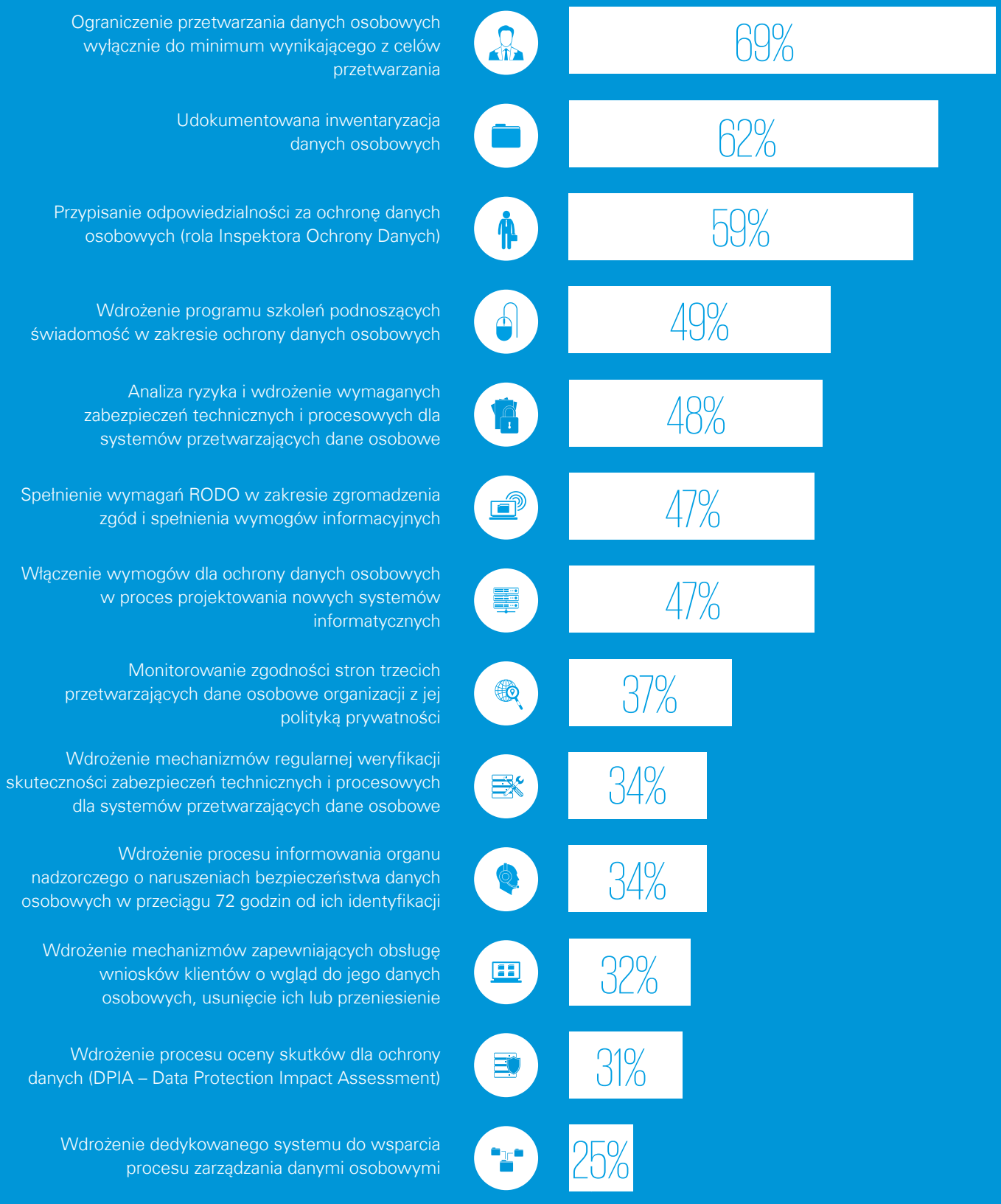
Jak firmy oceniają status przygotowań do zapewnienia zgodności z wymogami RODO?

Status przygotowań do RODO



Wdrożone rozwiązania zgodne z wymogami RODO

Które z poniższych rozwiązań zostały już w pełni wdrożone w organizacjach w celu zapewnienia zgodności z RODO?



Informacje o badaniu

Wielkość firm wg liczby zatrudnionych

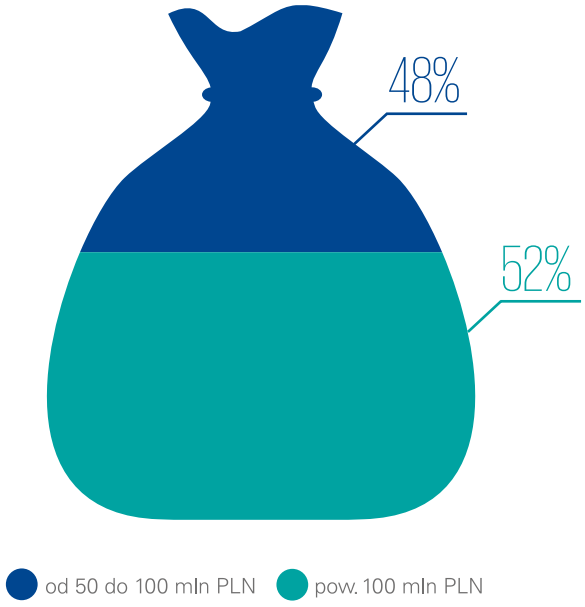
11% małe (max 49 osób)

51% średnie (50-249 osób)

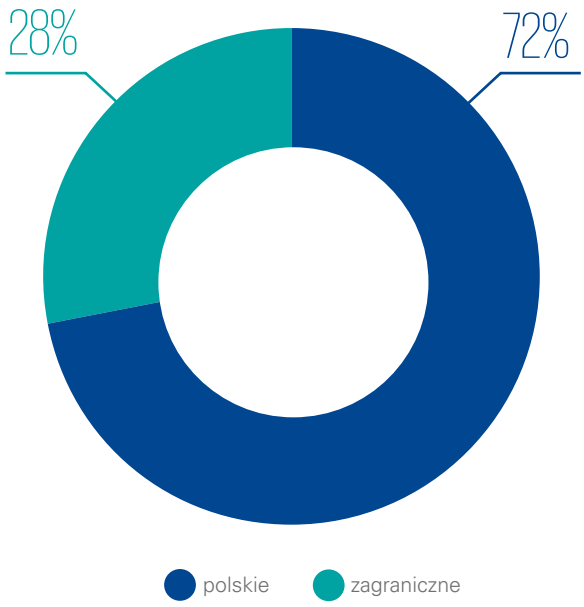
38% duże (pow. 250 osób)

Badanie zostało zrealizowane metodą wywiadów telefonicznych CATI wśród osób odpowiedzialnych za bezpieczeństwo IT w firmach (członków zarządu, dyrektorów ds. bezpieczeństwa, prezesów, dyrektorów IT lub innych osób odpowiedzialnych za ten obszar). Badanie zostało zrealizowane na próbie 101 organizacji na przełomie listopada i grudnia 2017 roku przez firmę Norstat Polska.

Roczne przychody firm

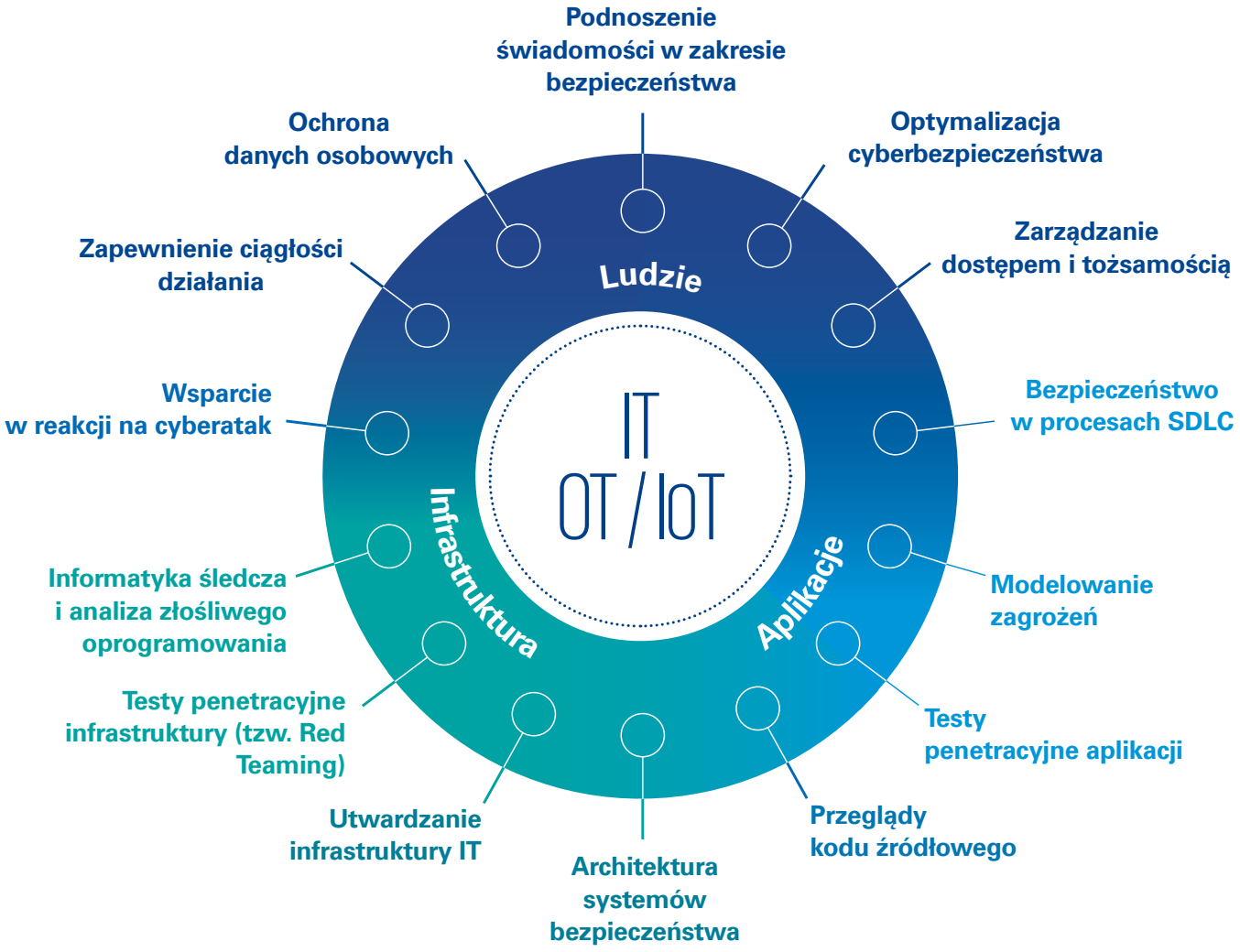


Pochodzenie kapitału



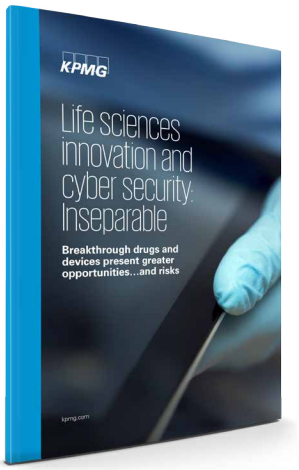
Usługi KPMG w zakresie cyberbezpieczeństwa

Zespół Cyberbezpieczeństwa KPMG świadczy szeroki zakres usług, podchodzący w kompleksowy sposób do ochrony informacji. Wspiera firmy w zabezpieczeniu infrastruktury, aplikacji oraz zadbaniu o czynnik ludzki, czyli właściwą organizację, procesy oraz wiedzę pracowników w zakresie ochrony informacji. Pomaga firmom zarówno w przygotowaniu się na odparcie cyberataku, jak również w podjęciu właściwych działań, gdy cyberatak już nastąpił.



Wybrane publikacje KPMG w Polsce i na świecie

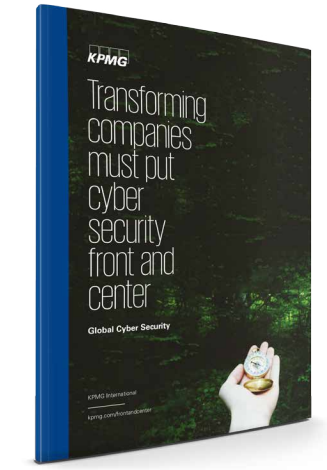
Cyberbezpieczeństwo – wyzwanie współczesnego prezesa



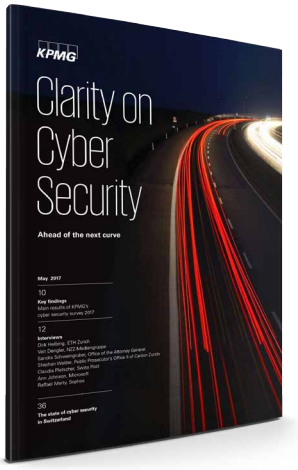
Life science innovation and cyber security: Inseparable

Cyber security for the fourth industrial revolution

Embracing the cyber insurance opportunity



Transforming companies must put cyber security front and center



Clarity on Cyber Security

Kontakt

KPMG w Polsce
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

Michał Kurek
Usługi doradcze
Cyberbezpieczeństwo
Partner
E: michalkurek@kpmg.pl

Krzysztof Radziwon
Usługi doradcze
Zarządzanie Ryzykiem
Partner
E: kradziwon@kpmg.pl

Magdalena Maruszczak
Marketing i Komunikacja
Dyrektor
E: mmaruszczak@kpmg.pl

KPMG.pl

Biura KPMG w Polsce

Warszawa
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

Kraków
ul. Opolska 114
31-323 Kraków
T: +48 12 424 94 00
F: +48 12 424 94 01
E: krakow@kpmg.pl

Poznań
ul. Roosevelta 22
60-829 Poznań
T: +48 61 845 46 00
F: +48 61 845 46 01
E: poznan@kpmg.pl

Wrocław
ul. Szczytnicka 11
50-382 Wrocław
T: +48 71 370 49 00
F: +48 71 370 49 01
E: wroclaw@kpmg.pl

Gdańsk
al. Zwycięstwa 13a
80-219 Gdańsk
T: +48 58 772 95 00
F: +48 58 772 95 01
E: gdansk@kpmg.pl

Katowice
ul. Francuska 34
40-028 Katowice
T: +48 32 778 88 00
F: +48 32 778 88 10
E: katowice@kpmg.pl

Łódź
al. Piłsudskiego 22
90-051 Łódź
T: +48 42 232 77 00
F: +48 42 232 77 01
E: lodz@kpmg.pl