

[www.pwc.co.uk](http://www.pwc.co.uk)

## ***Więcej niż świadomość: rosnące znaczenie zarządzania danymi wśród europejskich firm średniej wielkości***

Badanie postaw, zachowań i najlepszych praktyk w europejskich przedsiębiorstwach, w tym zaktualizowany Wskaźnik Świadomości Ryzyka Informacyjnego

*Raport PwC we współpracy z Iron Mountain  
Czerwiec 2013*



**pwc**





## ***Spis treści***

---

### ***Wstęp***

---

***i        Streszczenie***

---

***1        Stan zagrożenia informacyjnego dziś***

---

***5        Konieczność zarządzania rosnącym bagnem danych***

---

***7        Obowiązek kształcenia pracowników: czy można ufać zaufanym?***

---

***9        Wartość informacji***

---

***11       Przyjęcie najlepszych praktyk***

---

***14       Załącznik: Metodologia badań***

---

***17       Autorzy raportu***

---

# Wstęp



Christian Toon  
Dyrektor ds. ryzyka  
informacyjnego

## Poruszanie się w świecie informacji

Krajobraz informacyjny w Europie przeszedł kompletną metamorfozę. Każdy sektor w każdym kraju boryka się z dostosowaniem do tej zmiany. Wiele przedsiębiorstw ma wątpliwości, jak radzić sobie z gwałtownie rosnącą ilością informacji w wielu formatach, nagłym rozwojem mediów społecznych, rozpowszechnieniem urządzeń mobilnych, zmianami w przepisach i rosnącym zagrożeniem ze strony złośliwego oprogramowania. Jednocześnie obserwujemy zwiększone zainteresowanie zagospodarowaniem wartości usystematyzowanych i nieusystematyzowanych informacji. W efekcie zarządzanie informacją to dziś bardziej złożona kwestia niż kiedykolwiek wcześniej, a wraz ze wzrostem złożoności zwiększa się ryzyko.

Dlatego też Iron Mountain i PwC podjęły się zbadania poziomu zagrożenia informacji w średnich przedsiębiorstwach w Europie w odpowiednim momencie. Wskaźnik świadomości ryzyka informacyjnego wyliczany jest po raz drugi. Po zbadaniu danych wyłania się pozytywny obraz postępów dokonanych w ciągu ostatnich 15 miesięcy. Świadomość ryzyka informacyjnego rośnie, co obrazuje wzrost wskaźnika wśród firm. Przeciętny wynik dla Europy wzrósł z 40,6 w ubiegłym roku do 56,8 na 100-punktowej skali. Nasze badania wskazują, że wyższy poziom świadomości przekłada się na niepewność, ponieważ przedsiębiorstwa widzą potrzebę działania, ale nie są pewne, gdzie się zwrócić i co robić dalej.

Teraz potrzebne jest przekucie podwyższonego poziomu świadomości na strategię i zestaw działań mających na celu ograniczenie ryzyka informacyjnego. Będzie to wymagało zainteresowania i zaangażowania na najwyższym szczeblu przedsiębiorstwa. Osoby odpowiedzialne za zarządzanie informacją muszą nauczyć się języka właściwego dla sali konferencyjnej i otworzyć się na dialog z innymi kluczowymi podmiotami. Utrata lojalności klientów, szkoda dla reputacji marki i spadek sprzedaży oraz przychodów to kluczowe obawy osób zarządzających informacjami, a wspomniane kwestie powinno z łatwością dać się przenieść na poziom zarządu. Jest jednak jasne, że jeśli ma dojść do prawdziwego postępu, przedsiębiorstwo powinno martwić się nie tylko ryzykiem dla reputacji i lojalności klientów, ale również dążyć do uświadomienia sobie możliwości i wartości, które mogą zostać odblokowane, gdy informacje są dobrze zarządzane, jako majątek przedsiębiorstwa.

Podczas opracowywania niniejszego dokumentu mieliśmy na celu nie tylko zrozumieć skalę i złożoność problemu, ale również przygotować coś pożytecznego dla europejskich przedsiębiorstw. Wskaźnik ryzyka i narzędzie oceny ryzyka online [www.ironmountain.co.uk/risk-assessment](http://www.ironmountain.co.uk/risk-assessment) zostały stworzone w celu dostarczenia przedsiębiorstwom informacji, które pomogą im zrobić kolejny krok na drodze do zarządzania ich informacjami w sposób odpowiedzialny. To studium przedstawia szereg działań, które pozwolą firmom usprawnić swoje podejście, a tym samym zmniejszyć poziom narażenia ich informacji oraz pomóc im wykorzystać wartość informacji, które są w ich posiadaniu.

# Streszczenie

*„Mówiąc wprost, przedsiębiorstwa średniej wielkości w Europie nie cenią wystarczająco posiadanych informacji, ani nie rozumieją ich wartości jako majątku przedsiębiorstwa.”*

Claire Reid, partner, dział bezpieczeństwa informacyjnego PwC

Przedsiębiorstwa borykają się z zarządzaniem informacjami w ich posiadaniu i są w związku z tym narażone na bezprecedensowy poziom ryzyka. Oszustwa, naruszenia bezpieczeństwa danych i katastrofy w mediach społecznościowych rozwijają się szybciej niż przedsiębiorstwa są w stanie reagować.

Przedsiębiorstwa średniej wielkości w Europie są szczególnie narażone, ale pozostają bierne w zakresie swoich praktyk zarządzania danymi. Nasze opracowanie pokazuje, że zamieszanie wokół tego, co robić dalej powstrzymuje przedsiębiorstwa średniej wielkości przed podjęciem działań na rzecz ochrony ich interesów oraz uświadomieniem sobie wartości posiadanych informacji.

## Najważniejsze wnioski z badania:

Świadomość nie jest już problemem. Nasze badanie pokazuje, że wśród przedsiębiorstw średniej wielkości rośnie poziom świadomości zagrożenia związanego z ryzykiem informacyjnym i konieczności podjęcia działań.

- Przeciętny wynik wskaźnika w tym roku to 56,8 z maksimum 100. Jest to krok naprzód w porównaniu z zeszłorocznym wynikiem (40,6), gdy niewiele podmiotów zarządzało swoimi informacjami na zadowalającym poziomie. Choć zaszła pewna poprawa, wskaźnik jest nadal niski i pozostaje wiele do zrobienia nim postępowanie w zakresie zarządzania danymi osiągnie odpowiedni poziom.
- 68% uważa, że odpowiedzialne podejście do informacji jest kluczem do sukcesu w biznesie. Informacje, w formie papierowej i cyfrowej, dotyczące klientów i wewnętrzne, są postrzegane jako cenne aktywa, a odpowiedni nadzór nad nimi może umożliwić realizację niewykorzystanych korzyści komercyjnych (a także pomóc w uniknięciu katastrofy).
- Wyniki badania sugerują, że przedsiębiorstwa są albo niepewne co do dalszych kroków, albo pozostają słabo przygotowane do radzenia sobie z zagrożeniem. Tylko 45% z nich dysponuje strategią ds. ryzyka informacyjnego i monitoruje jej skuteczność, a jednocześnie 44% spodziewa się wzrostu ryzyka naruszenia danych.

## Wyzwanie zarządzania informacjami:

Nasze badanie pokazuje, że wiele z nich grzęźnie w coraz większym „bagnie” niesklasyfikowanych danych w formacie tradycyjnym i cyfrowym, z którymi nie wiedzą co zrobić. W rezultacie rośnie ryzyko naruszenia integralności danych wrażliwych i poufnych.

- 36% zachowuje na wszelki wypadek wszystkie informacje.
- 42% martwi się o bezpieczeństwo swoich przechowywanych danych.

Wyłania się obraz pełen zamieszania, sprzeczności i bierności w zakresie zarządzania ryzykiem informacyjnym wśród przedsiębiorstw średniej wielkości. Coraz bardziej rośnie przepaść między nastawieniem i działaniami.



*„93% przedsiębiorstw zatrudniających więcej niż 250 pracowników doświadczyło naruszenia integralności danych w ciągu ostatniego roku. W najgorszym wypadku średni koszt każdego naruszenia wynosił między 450 000 i 850 000 funtów”.*

Źródło: PwC Information Security Breaches Survey 2013

- 78% wierzy, że należy robić wszystko, aby zapobiec naruszeniu danych, a mimo to 47%, rozczarowująca liczba, twierdzi, że ich zarząd nie postrzega ochrony danych jako istotnej kwestii.
- Przedsiębiorstwa średniej wielkości wymagają od swoich dostawców najwyższych standardów bezpieczeństwa. Tylko 14% pracowało z firmą, która doświadczyła naruszenia integralności danych, ale same przedsiębiorstwa nie trzymają tych samych standardów.
- Kierownictwo średniego i niższego szczebla oraz personel pomocniczy obdarza się wysokim poziomem zaufania przy braku skutecznych, monitorowanych zasad i mechanizmów kontroli mających na celu zabezpieczenie danych. Na przykład, 58% nie monitoruje swoich systemów kontroli dostępu do informacji.

W niniejszym dokumencie skupiamy się na postawach i zachowaniach, które wyszły na jaw w naszej pracy. Wyróżniamy kilka kluczowych czynników, które hamują średnie przedsiębiorstwa przed zrealizowaniem w całości swojego potencjału.

#### **Najlepsze praktyki służące ograniczeniu ryzyka informacyjnego:**

Opierając się na ubiegłorocznym raporcie, zidentyfikowaliśmy szereg czynności i działań, które pomogą przedsiębiorstwom średniej wielkości naprawdę rozwinąć skrzydła i czerpać korzyści handlowe, które idą w parze z ochroną i docenieniem jednego z najcenniejszych aktywów przedsiębiorstwa - informacji na papierze i w formie cyfrowej. Działania te opisują następujące punkty:

- **Mierz wysoko** - poszukuj wsparcia na poziomie zarządu poprzez przyjęcie strategicznego podejścia wobec zarządzania informacjami.
- **Przejmij kontrolę nad tym, co masz** - wiedz jakie informacje posiadasz, gdzie są i zdecyduj, czy nadal są potrzebne.
- **Zaangażuj swoich ludzi** - prowadź politykę kontrolowanego zaufania opartą na zestawie narzędzi do monitorowania, zasad i procedur.

# Stan zagrożenia informacyjnego na dziś

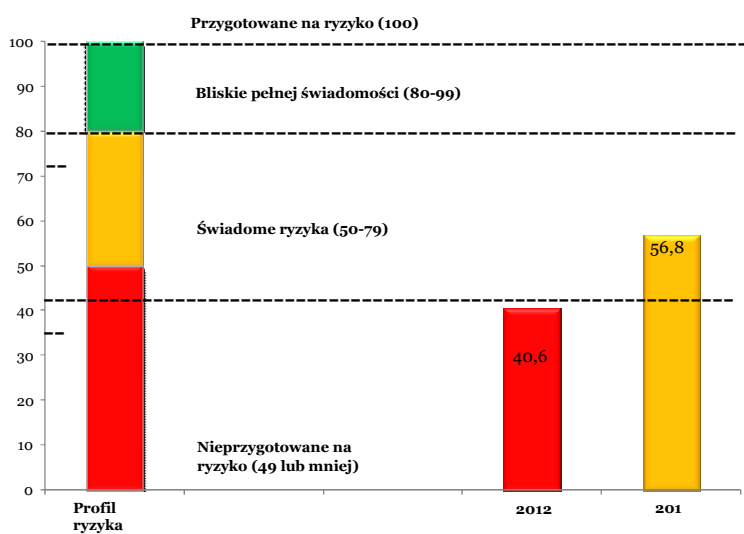
Przesłanie jest jasne: każda organizacja w posiadaniu informacji wymagających ochrony, niezależnie od wielkości i sektora, jest zagrożona. W czasach, gdy liczba naruszeń bezpieczeństwa danych, cyberataków i katastrof w mediach społecznościowych utrzymuje się na najwyższym poziomie w historii, przedsiębiorstwa są narażone na bezprecedensowe ryzyko. Mimo to firmy średniej wielkości nie chronią się przed nieodwracalnymi szkodami, które może spowodować naruszenie danych.

Spoczęcie na laurach, sprzeczne zachowania, złe praktyki zarządzania danymi i brak świadomości wartości informacji to nie tylko ryzyko dla przedsiębiorstw. Powstrzymują je przed osiągnięciem pełnego potencjału na rynku. Widoczny jest ewidentny brak zaufania do organizacji, które doświadczyły naruszenia danych, a te, które potrafią wykazać się właściwym podejściem wobec danych osiągną znaczną przewagę konkurencyjną.

Z naszego ostatniego badania, zleconego przez Iron Mountain, wynika, że średnie przedsiębiorstwa wciąż nie traktują właściwie swoich danych. Choć istnieją dowody pewnej poprawy w zakresie praktyk zarządzania danymi wśród europejskich firm średniej wielkości, niezadowolające postępowanie z danymi jest wciąż szeroko rozpowszechnione. PwC przeprowadził drugie z corocznej serii badań 600 przedsiębiorstw średniej wielkości (zatrudniających 250-2500 pracowników, zdefiniowanych jako średnie) w sześciu krajach europejskich: Wielkiej Brytanii, Francji, Niemczech, Holandii, Hiszpanii i na Węgrzech. Niniejszy dokument opiera się na ustaleniach z naszego opublikowanego w 2012 roku raportu Beyond Cyber Threats [„Więcej niż cyberataki”], w którym wprowadzony został po raz pierwszy w Europie Wskaźnik Ryzyka Informacyjnego i podkreślono potrzebę lepszego przygotowania średnich przedsiębiorstw do zarządzania ryzykiem informacyjnym.

Wynik za 2013 rok wskazuje na pewną poprawę w praktykach bezpieczeństwa informacyjnego wśród średniej wielkości przedsiębiorstw, ale przy wyniku 56,8 pozostaje wiele do zrobienia.

## Wskaźnik świadomości ryzyka informacyjnego 2012-2013.



### „Zakresy” świadomości ryzyka

#### Przygotowane na ryzyko

Przedsiębiorstwa wdrożyły odpowiedzialne podejście, obejmujące strategię, ludzi, komunikację i bezpieczeństwo na wszystkich poziomach. Monitorują, oceniają i poprawiają swoje podejście do efektywnego zarządzania ryzykiem.

#### Bliskie pełnej świadomości

Przedsiębiorstwa określiły pewne działania i istnieje podwyższona świadomość u kierownictwa wyższego szczebla. Zredukowały swój poziom narażenia na ryzyko, ale nie wdrożyły solidnej strategii.

#### Świadome ryzyka

Przedsiębiorstwa obudziły się i zdają sobie sprawę z konieczności zarządzania ryzykiem. Jednak nie są pewne, co robić lub pozostają słabo przygotowane do uporania się z zagrożeniem.

#### Nieprzygotowane na ryzyko

Przedsiębiorstwa są poważnie narażone na ryzyko informacyjne. Prawdopodobieństwo, że dysponują strategią ds. ryzyka informacyjnego jest niskie, a kierownictwo wyższego szczebla nie zdaje sobie sprawy z potencjalnego jego wpływu na działalność.

PwC

Baza: 600

## ***Bierność średnich przedsiębiorstw trwa...***

Tylko 45% z nich dysponuje strategią ds. ryzyka informacyjnego i monitoruje jej skuteczność.

Tylko 38% ma formalny plan naprawczy dla przedsiębiorstwa.

Tylko 32% sprawuje nadzór nad skutecznością swojego rejestru ryzyka korporacyjnego.

Tylko 28% prowadzi i ocenia programy komunikacji z pracownikami zorientowane na utrwalenie procedur dot. ryzyka informacyjnego.

Tylko 45% monitoruje skuteczność zespołu ds. ryzyka informacyjnego.

Tylko 39% monitoruje skuteczność klasyfikacji danych.

Tylko 26% ocenia zwrot z inwestycji w bezpieczeństwo informacji.

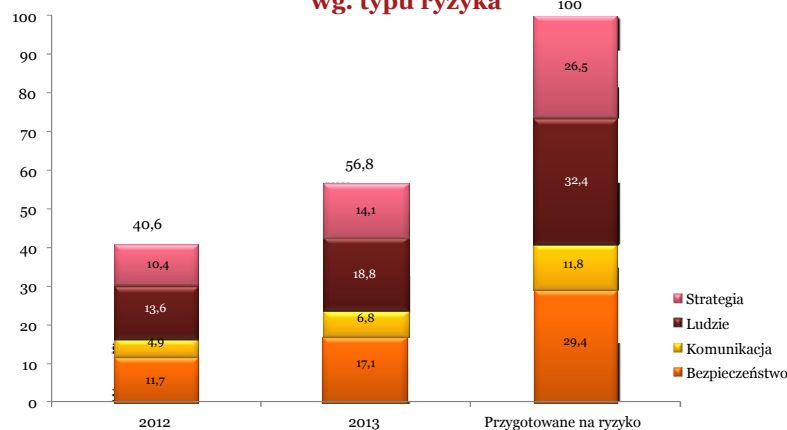


*„Przedsiębiorcy muszą przyjąć nowy sposób myślenia. Taki, w którym bezpieczeństwo informacji to jednocześnie środek służący ochronie danych i możliwość tworzenia wartości dla firmy.”*

PwC Badanie globalnego stanu bezpieczeństwa informacji 2013

Średnie przedsiębiorstwa są już poza strefą zagrożenia, ale powinny nadal zwracać uwagę na poziom ryzyka, na które są narażone. W świecie, w którym prawdopodobieństwo naruszenia danych rośnie lawinowo z dnia na dzień, firmy muszą wdrażać lepsze plany w celu zapewnienia sobie ochrony. Nie ma powodu, by przedsiębiorstwa nie dążyły do uzyskania maksymalnej liczby punktów (100), co oznaczałoby, że są przygotowane na ryzyko.

### **Wskaźnik świadomości ryzyka informacyjnego 2012-2013 – analiza wg. typu ryzyka**



Aby osiągnąć wynik 100, przedsiębiorstwa muszą wdrożyć i monitorować skuteczność 34 określonych na potrzeby wyliczenia wskaźnika środków (opisanych w załączniku do niniejszego dokumentu). Żaden z nich nie jest, naszym zdaniem, trudny do wprowadzenia lub monitorowania, ale nasze badania wskazują, że przed przedsiębiorstwami średniej wielkości jeszcze długa droga, a one zdają się zagubione w odniesieniu do tego, co robić dalej.

Pozytywną oznaką jest bardziej sumienne obecnie monitorowanie przez średnie przedsiębiorstwa skuteczności ich praktyk zarządzania informacjami, zwłaszcza w dziedzinie bezpieczeństwa danych. Widoczne jest również dodatkowe skupienie uwagi na ludziach. Jednakże, w szerszej perspektywie, około połowa przedsiębiorstw biorących udział w naszym badaniu musi jeszcze znacznie poprawić swoje praktyki zarządzania informacjami.



## Kluczowe wnioski

55% francuskich firm posiada monitorowaną strategię ds. ryzyka informacyjnego, w porównaniu do 34% przedsiębiorstw w Wielkiej Brytanii i 45% łącznie.

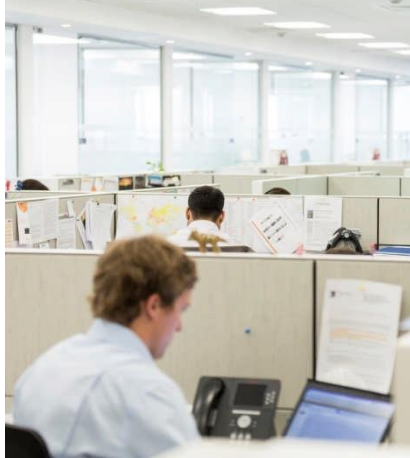
40% firm holenderskich i 38% węgierskich ma monitorowany rejestr ryzyka korporacyjnego, w porównaniu do 21% w Niemczech i 32% łącznie.

52% firm holenderskich posiada strategię bezpiecznej utylizacji sprzętu i poufnych dokumentów. Taka procedura funkcjonuje tylko w 26% hiszpańskich przedsiębiorstw i 41% łącznie.

61% na przedsiębiorstwach na Węgrzech i 59% w Holandii dysponuje jasnymi wytycznymi dla pracowników dotyczącymi bezpiecznego usuwania dokumentów, w porównaniu do 50% łącznie i 36% w Hiszpanii.

35% firm w sektorze prawniczym posiada monitorowaną strategię ryzyka informacyjnego wobec 55% przedsiębiorstw w sektorze ubezpieczeniowym i 45% łącznie

54% firm produkcyjnych i inżynierskich ma specjalny zespół ds. ryzyka informacyjnego. 34% firm prawniczych posiada taki zespół, wobec 45% łącznie.



PwC

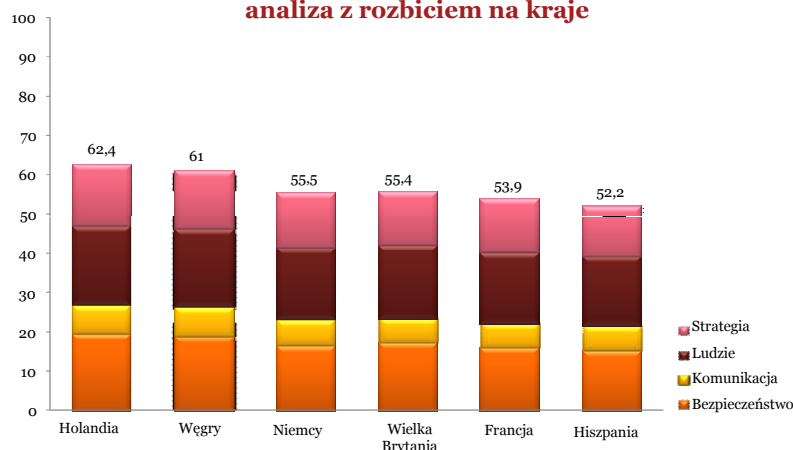
Kluczowy obszar do poprawy to brak strategicznego zorientowania na zarządzanie informacjami. Ponad połowa firm nie monitoruje skuteczności swojej strategii ryzyka informacyjnego, jeśli taką strategię posiada.

Średnie przedsiębiorstwa muszą się obudzić i zdać sobie sprawę, że informacje są aktywem o krytycznej wartości dla firm i muszą być odpowiednio traktowane oraz zarządzane. W okresie recesji jest to jeszcze ważniejsze. Zrobić więcej przy zaangażowaniu mniejszych środków można tylko pracując w sposób bardziej inteligentny, nie tylko ciężiej, a odnoszące największe sukcesy organizacje osiągają to nie tylko poprzez podejście do i korzystanie z informacji jako majątku, ale także określenie ich wartości. Zdały sobie sprawę, że dba się tylko o to co cenne.

## Różnice pomiędzy krajami

Holandia i Węgry osiągnęły najwyższe wyniki wskaźnika, odpowiednio 62,4 i 61,0, przy czym w przypadku Holandii zaobserwować można znaczącą poprawę w ciągu ostatniego roku.

**Wskaźnik świadomości ryzyka informacyjnego 2012-2013 - analiza z rozbiem na kraje**



Spośród sześciu krajów uczestniczących w naszym badaniu Holandia wyróżnia się jako kraj z najbardziej strategicznym podejściem do ryzyka informacyjnego. Na przykład, holenderskie przedsiębiorstwa częściej niż ich odpowiedniki w innych krajach dysponują planem awaryjnym na wypadek problemów z danymi na małą skalę, rejestrem ryzyka korporacyjnego, strategią obejmującą telefony komórkowe, a także urzędzenia osobiste i bezpieczeństwo komputerów przenośnych oraz strategią bezpiecznej utylizacji sprzętu i dokumentów poufnych. Ponadto, Holandia, a także Francja, to kraje w których ryzyko informacyjne najprędzej stanowi kwestię omawianą na poziomie zarządu.

Na Węgrzech główne usprawnienia związane są z działaniami szkoleniowymi dla pracowników i komunikacją, z silnym naciskiem na dostarczanie pracownikom zaleceń co do przechowywania i usuwania dokumentów elektronicznych oraz fizycznych.

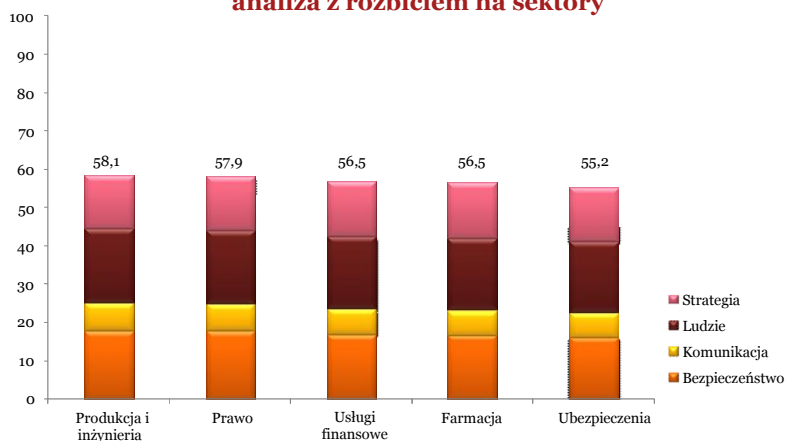
Hiszpania z kolei osiągnęła najniższy wynik - 52,2. Co ciekawe, w przypadku hiszpańskich firm prawdopodobieństwo postrzegania pracowników jako zagrożenia dla bezpieczeństwa informacji jest najniższe. Jednocześnie ich wynik jest słabszy w porównaniu do europejskich odpowiedników w odniesieniu do udzielania pracownikom wskazówek na temat polityk i procedur wewnętrznych, jak również najniższe jest w ich przypadku prawdopodobieństwo wdrożenia niektórych z kluczowych środków bezpieczeństwa, takich jak programy należytej staranności w zakresie postępowania z danymi osobowymi, klientów lub pracowników, systemy wykrywania włamań i uznane systemy klasyfikacji danych.



## Różnice pomiędzy sektorami

W ujęciu sektorowym, wszystkie pięć sektorów w naszym badaniu poczyniło postępy i znajdują się na podobnym poziomie przygotowania, a jednocześnie pozostają w dolnej części strefy „burszynowej”.

**Wskaźnik świadomości ryzyka informacyjnego 2012-2013 - analiza z rozbiciem na sektory**



Sektor usług prawnych oraz produkcyjny i inżynierski wykazały największy wzrost od 2012 roku. Istnieją dowody na to, że firmy produkcyjne i inżynierskie w coraz większym stopniu przyjmują bardziej strategiczne podejście. Więcej z nich posiada strategię ds. ryzyka informacyjnego i formalny plan naprawczy firmy. W sektorze tym o wiele większe jest również prawdopodobieństwo postrzegania pracowników jako zagrożenia dla bezpieczeństwa informacji, a w porównaniu do ubiegłego roku widać zwiększony nacisk na środki dotyczące osób i komunikacji.

Przedsiębiorstwa z branży prawnej poprawiły wyniki w zakresie większości z 34 środków, ale w dalszym ciągu ze wszystkich sektorów to właśnie w tym najniższe jest prawdopodobieństwo posiadania strategii ds. ryzyka informacyjnego lub specjalnego zespołu/osoby odpowiedzialnej za ryzyko informacyjne.

**Wskaźnik świadomości ryzyka informacyjnego  
Ranking według kraju: 2012 - 2013.**

Kraj	2012	2013
Holandia	5	1
Węgry	1	2
Niemcy	4	3
Wielka Brytania	6	4
Francja	3	5
Hiszpania	2	6

# Konieczność zarządzania rosnącym bagnem danych

*„W dzisiejszym hybrydowym świecie informacji cyfrowych i papierowych istnieje ryzyko utonięcia firm w bagnie komplikacji i zamieszania, chyba że zajmą się swoimi informacjami. Odpowiedzialne podejście do informacji ma zasadnicze znaczenie, jeśli firmy chcą zrealizować korzyści z tego ważnego składnika aktywów biznesowych. Podejście takie ma kluczowe znaczenie, jeżeli przedsiębiorstwa mają zasłużyć na i zachować ciężko zdobytą reputację marki i lojalność klientów.”*

Christian Toon  
Dyrektor ds. ryzyka  
informacyjnego  
Iron Mountain

*„Co godzinę w Internecie przesyłane jest tyle informacji, by zappełnić 7 milionów płyt DVD. Położone obok siebie sięgałyby na wysokość Mount Everest 95 razy.”*

Badanie IMS dla IBM, 2013

Wiele przedsiębiorstw średniej wielkości powoli tonie w „bagnie” nieusystematyzowanych danych, z którymi nie wiedzą jak postępować. Wspomniane bagno danych powstało w wyniku niewdrożenia polityk, procesów i technologii służących kategoryzowaniu informacji oraz nieokreślenia potrzebnych informacji i sposobu ich przechowywania oraz tego, co może zostać zniszczone. W rezultacie wiele przedsiębiorstw przechowuje wszystkie informacje w formie cyfrowej i papierowej, co często oznacza, że duże ilości danych poufnych i wrażliwych są dostępne dla pracowników lub kontrahentów, co zwiększa prawdopodobieństwo naruszenia danych.

Ponad jedną trzecią przedsiębiorców z naszego badania przechowuje na wszelki wypadek wszystkie swoje dane. Kolejna jedna trzecia potrzebuje zasięgnąć porady prawnej przed podjęciem decyzji co do postępowania z danymi. Powszechnie wiadomo, że ilość danych cyfrowych i na papierze powstających z roku na rok rośnie w postępie geometrycznym, więc jeśli firmy nadal będą przechowywać wszystko, zarządzanie rozrastającym się bagnem danych będzie kosztowne i może narazić przedsiębiorstwo na ryzyko. Na przykład, pewne rodzaje dokumentów należy odpowiednio zniszczyć, zgodnie z prawnie określonymi okresami przechowywania, i niedopełnienie tego obowiązku może prowadzić do nałożenia kar oraz zniszczenia reputacji firmy. Ponadto, wiele przedsiębiorstw obawia się o bezpieczeństwo przechowywanych danych. Ewidentnie, trzeba zarządzać dostępem do przechowywanych danych i wdrożone muszą zostać odpowiednie środki kontrolne w celu zapobieżenia naruszeniom danych.

Wzrost znaczenia danych cyfrowych, w różnych dostępnych zdalnie formatach, w tym rozpowszechnienie rozproszonych łańcuchów udostępniania danych, również służy stworzeniu środowiska, w którym przedsiębiorstwa średniej wielkości zmagają się z kontrolą „łańcucha odpowiedzialności”. Informacje biznesowe o krytycznym znaczeniu są teraz dostępne w wielu formatach, w wersjach cyfrowych i tradycyjnych, dla większych grup, ponownie zwiększając ryzyko naruszenia danych.

Im więcej informacji organizacja przechowuje, tym większe jest zagrożenie ze strony biernych, ciekawskich, niewyszkolonych, niezadowolonych lub złośliwych pracowników. Jak wskazano w *Beyond Cyber Threats*, jednym z największych zagrożeń dla integralności informacji w miejscu pracy jest zachowanie i postawy pracowników. Organizacje, w których rośnie liczba niesklasyfikowanych danych, niepomniernie zwiększają to zagrożenie.

**„90% danych na świecie stworzono w ciągu ostatnich dwóch lat”**

IBM  
Understanding Big Data - IBM Big Data Platform

*„Trzy czwarte  
pracodawców w  
Wielkiej Brytanii  
powiedziało, że nie  
posiada możliwości do  
wyegzekwowania  
systemu  
zapobiegającemu  
nieautoryzowanemu  
dostępowi ze strony  
pracowników do  
danych firmy.”*

UK Insider Threat Survey,  
LogRhythm. Kwiecień 2013

Nawet liderzy - przedsiębiorstwa w czołówce stawki w zakresie bezpieczeństwa danych – mają problemy z przechowywaniem danych. Z naszego badania wynika, że w ich przypadku prawdopodobieństwo przechowywania na wszelki wypadek wszystkich danych jest równie wysokie.

Z perspektywy krajów, największe bagno danych występuje we Francji, gdzie połowa przedsiębiorstw biorących udział w badaniu przechowuje wszystkie swoje dane. Firmy w Hiszpanii wykazują najniższy poziom przechowywania danych i najczęściej korzystają z usług firm zewnętrznych do zarządzania tym procesem.

To raczej kwestia braku pomysłu na dalsze postępowanie, a nie błogiej niewiedzy. Przy pytaniu o największe wyzwanie w przyszłości 41% wspomniało, że martwi się zarządzaniem swoim papierowym dziedzictwem. Dotyczyło to w szczególności Niemiec i Węgier, a także sektora prawniczego w całej Europie. We wspomnianych przypadkach prawie połowa zapytanych przedsiębiorstw widziała wyzwanie w zarządzaniu swoimi papierowymi dokumentami. Kolejne zmartwienie średnich przedsiębiorstw to bezpieczeństwo przechowywanych danych. Dotyczy to 42%, 48% we Francji i 52% w sektorze ubezpieczeniowym.

Oprócz skoncentrowania się na rozwijaniu właściwych zachowań wśród pracowników, firmy średniej wielkości powinny zająć się swoimi bagnami danych nim będzie za późno. Niezbędne jest zapoznanie się z przepisami i wytycznymi w zakresie przechowywania danych. Klasyfikowanie i bezpieczne zachowanie niezbędnych danych, jak również bezpieczne niszczenie zbędnych dokumentów to konieczność. Przedsiębiorstwa muszą działać teraz, nim bagno wymknie się spod kontroli i zacznie wyciekać.



## ***Kluczowe wnioski***

36% przechowuje wszystkie informacje na wypadek gdyby były potrzebne

31% zwraca się po pomoc prawną dotyczącą przechowywania danych przed podjęciem działań

41% postrzega „zarządzanie papierowym dziedzictwem” jako znaczące wyzwanie w przyszłości

42% martwi się o bezpieczeństwo swoich przechowywanych danych

61% nie monitoruje skuteczności swoich systemów klasyfikacji danych, o ile takie systemy posiadają



# Obowiązek kształcenia pracowników: czy można zaufać zaufanym?

## Kluczowe wnioski

Tylko 14% respondentów prowadziło interesy z organizacją, w której doszło do naruszenia integralności danych.

Tylko 25% widzi pracowników jako poważne zagrożenie dla bezpieczeństwa informacji

82% ufa, że pracownicy będą przestrzegali ich polityki ds. ryzyka informacyjnego

45% nie monitoruje użycia mediów społecznościowych przez pracowników

## Studium przypadku

Innowacyjny pomysł wyznaczenia „młodzieżowego” komisarza przez policję w Kent okazał się strzałem w stopę z powodu osobistych kont nastolatki w mediach społecznościowych. Siedemnastoletnia Paris Brown została wybrana spośród 160 zainteresowanych zostaniem „głosem młodych” dla policji w Kent. Później okazało się jednak, że wpisy na jej osobistym koncie na Twitterze na wiele miesięcy wstecz zawierały rasistowskie, homofobiczne i niecenzuralne treści. Komisarz policji w Kent przyznał, że kont nastolatki w mediach społecznościowych nie sprawdzono przed jej zatrudnieniem.

W postępowaniu firm średniej wielkości widoczne są oznaki zamieszania i sprzeczności w podejściu do ryzyka informacyjnego. Nasze badanie pokazuje, że 58% nie nawiązałoby współpracy z organizacją, w której doszło do naruszenia danych, ale wiele z nich nadal naraża swoje własne dane. Skoro tylko 45% posiada monitorowaną strategię ds. ryzyka informacyjnego, mamy w efekcie do czynienia z „podwójnym standardem” - czujności na zewnątrz wobec bierności wewnątrz.

Firmy średniej wielkości muszą zacząć stosować w odniesieniu do siebie te same normy, których używają przy wyborze dostawców i wykonawców. Nie widzą, że ich klienci będą prawdopodobnie postępowali tak samo i w przypadku naruszenia integralności danych nie nawiążą współpracy.

Zeszlóroczne badanie *Beyond Cyber Threats* podkreśliło znaczenie wprowadzenia stopniowych zmian w kulturze biznesowej i zachowaniu pracowników, jeśli aktywa informacyjne europejskich przedsiębiorstw średniej wielkości mają być chronione. Tegoroczne badanie pokazuje, że firmy są bardzo świadome wpływu naruszenia danych na ich działalność, ale nadal pozostają niewzruszone wobec zagrożeń z wewnątrz. Dla 25% przedsiębiorstw z którymi rozmawialiśmy pracownicy to poważne zagrożenie dla bezpieczeństwa informacji, a jednocześnie 82% ufa, że będą oni przestrzegali ich polityki ds. ryzyka informacyjnego (jeśli mają taką politykę).

Przedsiębiorstwa średniej wielkości wciąż mówią nam, że kierownik ds. bezpieczeństwa IT to główny strażnik ich informacji i osoba odpowiedzialna za ryzyko informacyjne w organizacji. Jak na ironię, na pytanie kto jest zmartwieniem jako największy czynnik ryzyka z punktu widzenia naruszenia danych ponad połowa odpowiedziała, że zespół IT. To zrozumiałe, że osoby z największą odpowiedzialnością i o najszerzym dostępie do najbardziej wrażliwych i poufnych danych są uważane za największe zagrożenie.

## Kto jest zmartwieniem jako największe ryzyko z punktu widzenia naruszenia danych?





*„80% pracodawców w Wielkiej Brytanii twierdzi, że nie wierzą, by którykolwiek z ich pracowników mógł wykraść poufne informacje, ale sondaż wśród pracowników pokazał, że 23% z nich uzyskało dostęp lub wzięło poufne dane ze swojego miejsca pracy.”*

*UK Insider Threat Survey,  
LogRhythm, kwiecień 2013*

Kierownicy średniego szczebla, pracownicy niższego szczebla, asystenci i personel sprzątający są według naszych badań postrzegani jako czynnik niskiego ryzyka dla naruszenia danych, prawdopodobnie ze względu na stosunkowo ograniczony dostęp. Jednak nawet najbardziej godni zaufania pracownicy mogą się pomylić, a mimo to wiele organizacji nie ma wdrożonych mechanizmów kontroli służących ochronie przed prostym błędem ludzkim. Na przykład, 61% firm nie monitoruje skuteczności swoich systemów klasyfikacji danych, a 58% nie posiada lub nie przeprowadza oceny swoich systemów kontroli dostępu do archiwów firmy i innych wrażliwych informacji.

W przypadku wielu przedsiębiorstw średniej wielkości stwierdzić można również brak procedur kontroli pracowników. Mniej niż połowa sprawdza referencje od pracodawców, a tylko 40% przeprowadza kontrole na policji lub sprawdza rejestry karne. Ponadto, niewiele z nich korzysta z łatwo i publicznie dostępnych informacji na portalach społecznościowych, takich jak Twitter. Wygląda na to, że wiele firm średniej wielkości obdarza znacznym zaufaniem osoby, o których niewiele wie. Wiele organizacjom brak również zaangażowania w komunikację i szkolenie pracowników w zakresie ich polityk i procedur (jeśli takie istnieją). Zamiast tego mają wielkie pokłady zaufania wobec pracowników.

Zaufanie do pracowników może być czymś dobrym, ale problemem jest to, że wiele z dotychczasowych naruszeń było spowodowanych przez błąd ludzki. Dlatego ważne jest posiadanie polityki kontrolowanego zaufania i wdrożenie odpowiednich polityk, szkoleń, komunikacji i kontroli bezpieczeństwa w celu ochrony informacji zarówno od złych zamiarów, jak i nieszczęśliwych wypadków.

W świecie wszechobecnych mediów społecznościowych, gdzie 88% klientów korzysta z tego samego urządzenia mobilnego do celów osobistych i do pracy (dane PwC), potencjalna szkodliwość jest ogromna i istnieje wiele na to wiele znanych przykładów.



### *Przeciętny złodziej danych to:*

- Obecny pracownik
- Mężczyzna
- w wieku 37 lat

*W około połowie zbadanych przypadków pracownik ukradł tajemnice handlowe, a następnie informacje natury gospodarczej (rozliczenia lub cenniki), a w 75% przypadków nie miał upoważnienia do danych, które ukradł.*

*Insider Data Theft: When Good Employees Go Bad*

# Wartość informacji

*Świat biznesu się zmienia i firmy we wszystkich krajach i w różnych branżach regularnie wymieniają się teraz informacjami ponad granicami przedsiębiorstwa, czy z partnerami biznesowymi, czy też osobistymi urządzeniami pracowników. Teraz to już nie tylko wyzwanie dla IT; liderzy muszą mieć pewność, że chronią coś, co jest najbardziej krytycznym czynnikiem wzrostu i reputacji organizacji.*

Andrew Miller, Dyrektor ds. bezpieczeństwa informacji PwC

Informacje to strategiczny zasób firmy i traktowanie ich w ten sposób może otworzyć drogę ku wielu różnym korzyściom handlowym, nie tylko zapewnić silną przewagę konkurencyjną. Niestety, mimo że większość średniej wielkości przedsiębiorstw wierzy, że postrzeganie informacji jako majątku firmy to „kolejny przełom”, niewiele z nich w widoczny sposób realizuje ten cel.

Firmy średniej wielkości są również bardzo świadome wpływu naruszenia integralności danych. Dwie trzecie respondentów uważa, że miałyby negatywny wpływ na zaufanie i lojalność klientów. Dodatkowym potwierdzeniem tego jest fakt, że większość przedsiębiorstw z naszego badania nie zaufałoby innym organizacjom, które doświadczyły naruszenia integralności danych. Około połowy uważa, że takie zdarzenie byłoby szkodliwe dla reputacji ich marki i wierzą, że zaszkodziłoby sprzedaży.

## Jaki wpływ na przedsiębiorstwo miałyby naruszenie bezpieczeństwa danych?



Ewidentnie to troska o lojalność klientów, a nie zgodność stanowi główny czynnik motywujący organizacje do lepszego zarządzania swoimi danymi.

## Kluczowe wnioski

59% uważa, że koszty właściwej ochrony ich danych są mniejszym obciążeniem niż ryzyko.

54% uważa, że tempo zmian jest oszałamiające i nigdy nie będą w stanie za nim nadążyć.

*„Poświęciliśmy ponad piętnaście lat i 100 milionów funtów na rozwój szybkich bezszczotkowych silników, które napędzają nasze odkurzacze i suszarki do rąk Airblade. Żądamy natychmiastowego zwrotu naszej własności intelektualnej.” Dokumenty sądowe Dyson na poparcie roszczenia szpiegostwa przemysłowego. Październik 2012*

---

*Członkowie UK Civil Service Sports Club, których jest 130 tysięcy w całym kraju, zostali poinformowani o tym, że ich imiona, adresy, daty urodzenia i numery ubezpieczenia zostały skradzione z centralnej komputerowej bazy danych. Dane wykorzystano następnie w oszustwach.*

*Daily Telegraph 27.11.2012*

Wiemy, że bierność to duży problem, ale co jeszcze ogranicza organizacje? Z naszych badań wynika, że największe wyzwanie dla europejskich średnich przedsiębiorstw to strategiczne aspekty zarządzania informacjami. Martwią się również o koszty i czują się przytłoczone tempem zmian.

Jedynie niewielka część z firm jest chociaż blisko traktowania swoich informacji jako majątku, a nawet mniejsza grupa faktycznie przypisuje im wartość. Większość (74%) nie mierzy, bądź nie wie jak mierzyć zwrot z inwestycji w bezpieczeństwo informacji. Wiele z nich nie posiada w ramach swojej organizacji zdolności i umiejętności potrzebnych do odpowiedniego zarządzania swoimi aktywami informacyjnymi i 35% widzi w tym wyzwanie. Jeśli ktoś nie wie jak coś zrobić, rzadko robi to dobrze.

Wsparciem dla naszych ustaleń są badania naukowe pokazujące, że firmy konsekwentnie nie doceniają wartości informacji, zarówno w kategoriach absolutnych, jak i relatywnie w stosunku do dóbr materialnych. W związku z powyższym przedsiębiorstwa muszą (a) inwestować, zarówno kapitał jak i czas, aby opracować skutecznie zintegrowane i nadzorowane programy zarządzania informacjami oraz (b) dokonać ponownej ewaluacji priorytetów zorientowanej na postrzeganie informacji jako wartości biznesowej, a nie z perspektywy kosztów i ryzyka.



# Przyjęcie najlepszych praktyk

*„Jedynym sposobem na zabezpieczenie danych w obiegu i w spoczynku jest opracowanie ogólnej strategii bezpieczeństwa informacji w oparciu o dobre zrozumienie zagrożeń dla działalności i realizacji warstwowego podejścia do monitorowania bezpieczeństwa, które obejmuje dane w całym ich cyklu życia.”*

Claire Reid  
Partner ds. bezpieczeństwa informacji PwC

Ustalenia wskazane w niniejszym raporcie to wyzwania, dotyczące całej branży. Na szczęście eksperci ds. bezpieczeństwa znajdują rozwiązania i działania, które mogą zmniejszyć ryzyko utraty danych. Naszym zdaniem następujące działania to niektóre z najbardziej skutecznych.

## **Krok 1: Mierz wysoko**

**Poszukuj wsparcia na poziomie zarządu poprzez przyjęcie strategicznego podejścia wobec zarządzania informacjami.**

• Opracuj skuteczną strategię ds. ryzyka informacyjnego i monitoruj jej skuteczność. Przyjmij usystematyzowane podejście do opracowania strategii, czyli:

- Określ, w jaki sposób dane są przechowywane, przenoszone i usuwane w sieciach wewnętrznych i zewnętrznych;
  - Określ niezbędne technologie, procesy i mechanizmy kontroli pracowników służące zarządzaniu informacjami na różnych etapach ich cyklu życia;
  - Opracuj i wdroż mechanizmy kontroli oparte na podstawowych zasadach z zakresu bezpieczeństwa, trwałości i niezawodności informacji;
  - Krzew na poziomie całej firmy kulturę odpowiedzialności za informacje. Pracuj ze swoim zespołem HR. Odgrywa wiodącą rolę w przeciwdziałaniu ryzyku informacyjnemu.
  - Nie zapomnij o papierze: proste kroki, w tym klasyfikacja dokumentów, bezpieczne przechowywanie i dostęp do niszczarek są pomocne w stworzeniu kultury firmowej niezbędnej dla osiągnięcia takiej stopniowej zmiany.
- 
- Umieść bezpieczeństwo informacji w porządku obrad Rady. Wpłyń na program Rady, mówiąc ich językiem i dowiadując się, co jest ważne dla jej członków. Istnieje związek między trwałą lojalnością klientów a postrzeganiem zarządzania i ochrony danych klientów przez organizację. Kierunek obrany przez zarząd w zakresie zachowań i działań może prowadzić do przewagi handlowej, jeżeli będzie skutecznie wdrożony i monitorowany.
  - Postrzegaj swoje dane jako składnik aktywów i pokazuj pracownikom, że to naprawdę ważne - umieść je w bilansie lub zasięgnij porady co do pomiaru zwrotu z inwestycji w bezpieczeństwo informacji. Oblicz ile kosztowałoby zastąpienie wszystkich danych.
  - Wprowadź kulturę współodpowiedzialności za zarządzanie informacjami wśród pracowników. Zadbaj o to, by pracownicy byli świadomi, że to również ich osobista odpowiedzialność.





## ***Krok 2: Przejmij kontrolę nad tym, co masz***

***Wiedz, jakie informacje posiadasz, gdzie są i zdecyduj, czy nadal są potrzebne***

- Łatwo jest wierzyć, że przechowywane dane to tylko informacje w formie elektronicznej, ale nie zapominaj o archiwach w tradycyjnym formacie i o tym, jak są one używane, jak również o innych potencjalnie stosowanych formatach.
- Zidentyfikuj sponsorów na wysokich stanowiskach wewnątrz firmy, aby propagowali odpowiedzialność informacyjną wśród wszystkich osób w całej organizacji.
- Zidentyfikuj posiadane zasoby, ilość pamięci z rozbiorem na typy plików lub bazy danych, liczbę rekordów fizycznych i/lub multimedialnych. Idealnym rozwiązaniem byłoby dokonanie klasyfikacji według funkcji w przedsiębiorstwie lub typu.
- Określ, gdzie się znajdują. Wewnątrz, u osoby trzeciej, w kraju, poza UE?
- Musisz określić, czym dysponujesz i gdzie to się znajduje. Pozwoli to określić priorytety dla zarządzania ryzykiem i kosztami.
- Opracuj i rozpowszechnij proces zarządzania informacjami, który musi obejmować klasyfikację danych, protokół przechowywania, warunki dla przetwarzania danych, przechowywania danych lub zasady oceny i wykonywania kopii zapasowych.
- Okresy przechowywania informacji są kluczowym czynnikiem w zarządzaniu kosztami i zgodnością. Nie należy ich przechowywać dłużej niż to potrzebne.
- Kiedy dostępna będzie już polityka klasyfikacji, zadaj o to, by określić proces kontroli dostępu do dostępu do wrażliwych informacji i ograniczenia w zakresie przenoszenia dużych ilości danych.
- Wprowadź okres „amnestii” dla pracowników wewnętrznych, aby dać im czas na dostosowanie i postępowanie zgodne z modelem zarządzania informacjami. Oznaczałoby to, że pracownicy albo przechowują dane na dedykowanych serwerach pamięci masowej, albo pozbywają się niepotrzebnych już lokalnych danych.
- Nagradzaj pozytywne zachowanie i podejmuj działania w przypadku słabych wyników w zakresie zarządzania informacjami.
- Niech sponsorzy w ramach firmy monitorują i dokonują oceny Twojego modelu zarządzania informacjami.





### ***Krok 3: Zadbaj o to, by pracownicy byli z Tobą***

#### ***Prowadź politykę kontrolowanego zaufania***

- Ważne i korzystne jest, by liderzy w firmie mieli zaufanie do swoich pracowników. Jednak w obliczu rosnących zagrożeń (zarówno złośliwych i nieświadomych) zaufanie to musi być kontrolowane.
- Jest to określane na podstawie uzgodnionego zestawu narzędzi, zasad i procedur monitorowania, które stanowią podstawę i uzupełnienie nadrzędnego zaufania.
- Opracuj jasną politykę wykorzystania mediów społecznych dla pracowników i przeprowadź szkolenie, aby przekazać im odpowiednią wiedzę.
- Promuj wykorzystanie mediów społecznościowych za pośrednictwem odpowiednich kanałów, włącznie z jasnymi wytycznymi co do tego, co może, a co nie może być powiedziane.
- Określ konkretnie, co pracownicy mogą, a czego nie mogą pisać. Na przykład, zakaz publikacji "niewłaściwych komentarzy" jest zbyt ogólnikowy. Powiedz im, by nie wspominali nazw firm, konkretnych projektów i ludzi.
- Zachęcaj i umożliw pracownikom stanie się „czempionami” i ambasadorami marki, którzy mówiliby pozytywne rzeczy na temat przedsiębiorstwa jako miejsca pracy na swoich osobistych stronach w mediach społecznościowych.
- Przeprowadzaj kontrolowane ćwiczenia wewnętrzne z monitoringu, aby uzyskać wgląd w zachowanie pracowników w obliczu potencjalnego zagrożenia bezpieczeństwa.
- Komunikuj cel i charakter ćwiczeń z monitoringu i potraktuj je jako okazję do kształcenia pracowników w zakresie reakcji w przypadku naruszenia danych.
- Postępuj w bardziej zdyscyplinowany sposób w zakresie sporządzania, systematyzowania i przechowywania poufnych danych. Przykładem tego jest znakowanie dokumentów poufnych i opracowywanie takich dokumentów wzorcowych, by możliwe było ich wychwycenie przy wyprowadzeniu z organizacji (poprzez narzędzia zapobiegania utracie danych).
- Kontroluj wiadomości e-mail wysyłane na osobiste adresy poprzez wdrożenie kontroli na bramce e-mail.

# Załącznik: Metodologia badań



## Wstęp

Na poparcie ustaleń publikacji PwC i Iron Mountain opracowały solidną metodologię przeprowadzenia badań. Metodologia ta została opracowana na podstawie spostrzeżeń i doświadczeń zdobytych w ramach badania 2012. W pierwszej kolejności, współpracowaliśmy blisko z Iron Mountain w celu dokonania oceny tematów, które pojawiły się w badaniu z 2012 roku i z pomocą tych spostrzeżeń opracowaliśmy kompleksowy kwestionariusz, który był w dużej mierze oparty na kluczowych tematach badania, pod względem zakresu i skuteczności podejść biznesu do zarządzania ryzykiem informacyjnym z punktu widzenia osób, komunikacji i bezpieczeństwa.

Uzupełnienie powyższego stanowił zestaw „określeń postawy”, które pozwalają uzyskać głębszy wgląd w powody dla takich praktyk, zarówno w ujęciu ogólnym, jak i na poziomie kraju. W celu zachowania porównywalności ogólne stwierdzenia stanowiące podstawę dla wskaźnika świadomości ryzyka pozostały niezmienione. Kwestionariusz został opracowany wewnątrz PwC, przez zespół specjalistów ds. badań, z pomocą wiedzy ekspertów i z wkładem zespołu ds. przeciwdziałania ryzyku w PwC pod kierownictwem Claire Reid.

Ściśle współpracowaliśmy z naszym partnerem w zakresie badań terenowych, Coleman Parkes, aby kwestionariusz był w formie umożliwiającej jego wprowadzenie do ich systemu wspomaganego komputerowo wywiadu telefonicznego (computer assisted telephone interviewing suite; CATI) i dostępny w językach ojczystych naszej bazy respondentów.

PwC

## Z kim rozmawialiśmy?

Respondentami badania telefonicznego byli zazwyczaj dyrektorzy generalni, finansowi, informacyjni i kierownicy w celu poznania perspektywy osób na wyższych stanowiskach i wglądu w charakter oraz zakres najpilniejszych zagrożeń informacyjnych i w to jak są zarządzane. Wywiady telefoniczne przeprowadzono w odpowiednich proporcjach respondentów z kluczowych rynków i sektorów, w celu przeprowadzenia analizy porównawczej o wysokim poziomie szczegółowości.

W celu pozyskania jak największej ilości wiedzy z niniejszego badania, rozpoczęliśmy od kompleksowego „pozyskania” danych poprzez uzupełnienie ustaleń ogólnych, w szczególności w zakresie konkretnych trendów rynkowych i branżowych. Analiza ta obejmowała również ocenę kluczowych zmian stwierdzonych między 2012 i 2013, popartych spostrzeżeniami i informacjami z określeń postawy. Postanowiliśmy również pozyskać informacje z naszej sieci ekspertów PwC w tej dziedzinie z każdego z krajów europejskich biorących udział w badaniu.

W podobny sposób jak w 2012 roku opracowaliśmy wskaźnik świadomości ryzyka informacyjnego. Wskaźnik ten został wyliczony poprzez zastosowanie średniej ważonej dla poszczególnych odpowiedzi firm na 34 stwierdzenia ujęte w badaniu. Te 34 stwierdzenia zostały pogrupowane w czterech obszarach biznesowych zdefiniowanych jako „strategia”, „ludzie”, „komunikacja” i „bezpieczeństwo” i skategoryzowane jak pokazano na następnej stronie.

### ***Które z poniższych elementów są wdrożone w Państwa organizacji?***



#### **Strategia**

1. Strategia lub podejście ds. ryzyka informacyjnego.
2. Formalny plan lub strategia naprawcza dla przedsiębiorstwa.
3. Plan awaryjny dotyczący reakcji na „wypadki” lub przypadki utraty danych na małą skalę.
4. Regularne przeglądy polityki prywatności.
5. Rejestr ryzyka korporacyjnego.
6. Strategia ds. bezpieczeństwa informacji osobistych obejmujących osobiste urządzenia mobilne i bezpieczeństwo komputerów.
7. Strategia zarządzania usystematyzowanymi i nieusystematyzowanymi informacjami w postaci cyfrowej i fizycznej w wielu lokalizacjach.
8. Strategia bezpiecznej utylizacji sprzętu i niszczenia dokumentów poufnych.
9. Strategia, czyniąca priorytetem dostęp do dokumentów o znaczeniu krytycznym i najwyższego ryzyka, które są wspominane najczęściej w zapytaniach z zakresu zgodności.

#### **Ludzie**

10. Konkretna osoba lub zespół odpowiedzialny za ryzyko informacyjne w organizacji.
11. Proces opuszczenia przedsiębiorstwa dla pracowników, który zapobiega kradzieżom lub kopiowaniu przez nich danych.
12. Programy szkoleniowe służące instruowaniu pracowników w kwestiach ryzyka informacyjnego.
13. Świadomość ryzyka Informacyjnego zawarta w szkoleniu wprowadzającym.
14. Programy szkoleń "odświeżających".
15. Skuteczne programy szkoleń z ryzyka informacyjnego w zakresie IT.
16. Kontrola historii personelu.
17. Kodeks postępowania dotyczący prawidłowego zachowania wszystkich pracowników.
18. Narzędzie do pomiaru zaufania pracowników względem skuteczności działań z zakresu ryzyka informacyjnego.
19. Polityka korzystania z Internetu dla wszystkich pracowników.
20. Polityka korzystania z mediów społecznościowych dla wszystkich pracowników (na przykład Facebook, Twitter i LinkedIn).



## ***Komunikacja***

21. Dostępność informacji o ryzyku dla wszystkich pracowników.
22. Programy komunikacji z pracownikami służące utrwaleniu procedur z zakresu ryzyka informacyjnego
23. Jasne wytyczne dla pracowników dotyczące wewnętrznych procedur bezpiecznego usuwania i przechowywania dokumentów fizycznych.
24. Jasne wytyczne dla pracowników dotyczące wewnętrznych procedur bezpiecznego usuwania i przechowywania dokumentów elektronicznych.

## ***Bezpieczeństwo***

25. Polityki firmowe w odniesieniu do właściwego zabezpieczenia, przechowywania i usuwania informacji poufnych.
26. Programy należytej staranności dotyczące obchodzenia się z informacjami osobistymi, klientów lub pracowników.
27. Spis miejsc przechowywania informacji.
28. Scentralizowana baza danych zarządzania informacjami z zakresu bezpieczeństwa.
29. Technologia podglądu systemów wykrywania włamań oraz systemów zapobiegania włamaniom.
30. Próby prowadzone przez strony trzecie, na przykład testy penetracyjne.
31. Jasne, aktualizowane i uznane klasyfikacje danych.
32. Procedury kontroli w zakresie dostępu do budynków, obszarów o ograniczonym dostępie, archiwów firmy i innych wrażliwych informacji.
33. Stosowanie różnych zasad i metod przechowywania danych, biorąc pod uwagę różne okresy przechowywania dokumentów i wymogi z zakresu ochrony danych.
34. Procesy zgłaszania incydentów, na przykład, jak rozpoznać coś, czego nie powinno w danym miejscu być.



---

## Autorzy raportu



### ***Claire Reid***

Partner, Dział przeciwdziałania ryzyku PwC

T: +44 (0)207 212 5513

M: +44 (0)7734 607594

[claire.reid@uk.pwc.com](mailto:claire.reid@uk.pwc.com)



### ***David Armstrong***

Partner, Dział badań międzynarodowych PwC

T: +44 (0)28 90 245454

M: +44 (0)7713 680266

[david.m.armstrong@uk.pwc.com](mailto:david.m.armstrong@uk.pwc.com)



### ***Julie McClean***

Starszy kierownik, Dział badań międzynarodowych PwC

T: +44 (0)28 90 245454

M: +44 (0)7738 313241

[julie.mcclean@uk.pwc.com](mailto:julie.mcclean@uk.pwc.com)



### ***Biju Mukund***

Starszy kierownik, Dział przeciwdziałania ryzyku PwC

T: +44 (0)207 213 1701

M: +44 (0)7850 907913

[biju.mukund@uk.pwc.com](mailto:biju.mukund@uk.pwc.com)



### ***Kieran Jones***

Starszy specjalista, Dział badań międzynarodowych PwC

T: +44 (0)28 90 245454

M: +44 (0)7845 635383

[kieran.p.jones@uk.pwc.com](mailto:kieran.p.jones@uk.pwc.com)



[www.pwc.com](http://www.pwc.com)

Niniejsza publikacja została opracowana wyłącznie do celów informacyjnych w zakresie bieżących kwestii i nie stanowi profesjonalnego doradztwa. Nie należy podejmować jakichkolwiek działań w oparciu o przedstawione w niniejszym dokumencie informacje bez uzyskania profesjonalnego doradztwa. Informacje zawarte w publikacji nie są poparte jakimkolwiek oświadczeniem lub gwarancją (wyraźną lub dorozumianą) co do dokładności lub kompletności informacji w publikacji i, w zakresie dozwolonym przez prawo, PricewaterhouseCoopers LLP, członkowie, pracownicy i przedstawiciele nie przyjmują odpowiedzialności za jakiegokolwiek konsekwencje wynikające z podjęcia działania lub jego braku w oparciu o informacje opublikowane w niniejszym dokumencie, ani za decyzje podjęte na ich podstawie.

© 2013 PricewaterhouseCoopers LLP. Wszelkie prawa zastrzeżone. W niniejszym dokumencie „PwC” odnosi się do PricewaterhouseCoopers LLP (spółki o ograniczonej odpowiedzialności w Wielkiej Brytanii), członka PricewaterhouseCoopers International Limited, którego każdy członek stanowi oddzielny podmiot prawny.