



**DOBRE PRAKTYKI: PRZEWODNIK DLA  
SEKTORA PUBLICZNEGO**

# MIARĄ SIŁY ORGANIZACJI JEST WYTRZYMAŁOŚĆ JEJ NAJSŁABSZEGO OGNIWA

**Jak uwzględnić zachowania ludzkie  
w wewnętrznym zarządzaniu ryzykiem**

# WPROWADZENIE

Zawirowania ostatnich kilku lat zmusiły organizacje do ponownego przemyślenia swoich strategii zarządzania ryzykiem, ze szczególnym uwzględnieniem zapewnienia długoterminowej odporności na zagrożenia (business resilience).

Sektor publiczny to doskonały przykład, w którym rosnąca presja na cyfrową dostępność informacji i sprawną komunikację między departamentami napędza bezprecedensową transformację. Ogromne ilości danych - od wniosków o zasiłek dla bezrobotnych po rejestry szczepień - oraz nowo zautomatyzowane workflow w połączeniu z przejściem na elastyczny system pracy, oznaczają mnożenie się luk w zabezpieczeniach działalności operacyjnej oraz posiadanych wrażliwych danych.

## CZY WIESZ, ŻE?

Według naszego badania<sup>1</sup> prawie połowa (46%) menedżerów danych zgłasza, że w wyniku pandemii doświadcza zwiększonego ryzyka związanego z danymi.

## Jak w takim razie uchronić swoją firmę w obliczu nasilających się ataków?

Jednym z kluczowych obszarów, któremu często nie poświęca się dostatecznej uwagi, są zagrożenia wewnętrzne, ze strony pracowników. Jakkolwiek w większości przypadków składają się na nie nieumyślne

zachowania i błędy ludzkie, mogą być one niezwykle kosztowne dla organizacji, nie wspominając o uszczerbku na reputacji firmy. W czasach tak szybkiej cyfryzacji, aby zaspokoić wewnętrzne i zewnętrzne wymagania, organizacje sektora publicznego mają więcej do stracenia niż inne. Dobitnie ilustruje to pandemia COVID-19, która doprowadziła do tego, że wiele działów zajmowało się znacznie większą ilością danych osobowych niż wcześniej, przy często przeciążonych zespołach, nieprzygotowanych do pracy zdalnej, a tym samym narażonych na zwiększony stres i ryzyko błędów w swoich wysiłkach na rzecz pomocy obywatelom.

W niedawno ogłoszonym raporcie przygotowanym przez IBM średni koszt naruszenia ochrony danych **wzrósł z 1,08 mln USD do 1,93 mln USD** (ponad 79%) w ciągu ostatniego roku<sup>2</sup>.

Z tego względu Iron Mountain zlecił przeprowadzenie ogólnoeuropejskiego badania<sup>1</sup> wskazującego na potencjalne obszary, gdzie ludzkie słabości stanowią kluczowy czynnik w zarządzaniu ryzykiem w organizacji. Wyniki okazały się zaskakujące.

**Poniżej przedstawiamy spostrzeżenia i praktyczne wskazówki dotyczące zarządzania ryzykiem w zespołach pracujących w trybie hybrydowym i budowania odpornej na zagrożenia strategii biznesowej.**

1. Badanie 11 000 pracowników w 10 krajach, przeprowadzone we wrześniu 2021 r. przez One Poll.

2. Przygotowany przez IBM raport pt. „Koszty naruszenia ochrony danych” (Cost of a Data Breach), 2021 r.

## ROZDZIAŁY W PRZEWODNIKU

Zacznijmy od problemów, które łatwo rozwiązać.

**Oto kilka zaskakujących prawd o tym, jak pracujemy - w biurze i w domu.**

Jak wiele z nich występuje również w **Twojej** organizacji?



**Takie problemy można na szczęście rozwiązać stosunkowo prosto. Proponujemy rozważyć podjęcie następujących działań:**

- > Udostępnienie wyników ankiety w celu zwrócenia uwagi na problem bez "wskazywania palcem winnego"
- > Podkreślenie znaczenia zmiany zachowania
- > Wskazanie dostępnych narzędzi, szkoleń i wsparcia, które mogą pomóc
- > Przypomnienie, jaka jest różnica pomiędzy ryzykiem skalkulowanym a niepotrzebnym
- > Uaktualnienie polityki organizacji, aby zapewnić maksymalne zrozumienie problemu zarządzania ryzykiem oraz własnej odpowiedzialności za nie

## 2

**Choć nie można zmienić natury ludzkiej, można wpłynąć na sposób zarządzania ryzykiem w organizacji.**

Poprzez budowanie świadomej ryzyka kultury organizacyjnej od podstaw wspierany jest jednocześnie rozwój innowacji w firmie.

**Oto nasza rekomendacja pięciu kroków do zbudowania odporności organizacyjnej (business resilience) już na etapie projektowania.**

### 1 ZMIANA SPOSOBU MYŚLENIA W ORGANIZACJI

#### FAKTY:

Jeden na pięciu pracowników (22%) przyznaje się do **popelnienia „krytycznego” błędu w pracy**, a 10% podjęło ryzyko, które wiązało się z **poniesieniem kosztów** przez ich organizację.

#### ROZWIĄZANIE:

Warto zacząć od przyznania każdemu z pracowników funkcji ambasadora ryzyka, dzięki czemu świadomość ryzyka zostanie mocno **osadzona w kulturze organizacji**. Każdy pracownik powinien pamiętać, że świadomość ryzyka należy do jego kluczowych obowiązków.

OTO TWOJA  
**CHECK-LISTA!**  
ODHACZ OKIENKA  
PODZAS  
PLANOWANIA  
STRATEGII  
BIZNESOWEJ!

## 2

### PRZEKSZTAŁCENIE POLITYKI ZARZĄDZANIA INFORMACJAMI

#### FAKTY:

Ponad 1/3 (36%) wszystkich pracowników uważa, że **warto podejmować ryzyko zawodowe**, mimo że aż 21% z nich **padło ofiarą oszustwa lub phishingu**.

#### ROZWIĄZANIE:

W odpowiedzi na globalną pandemię COVID-19 organizacje sektora publicznego wdrożyły mechanizmy reagowania awaryjnego. Jednak obecnie w centrum uwagi pojawiły się długoterminowe strategie zbudowane wokół pracy hybrydowej. Należy się zastanowić, w jaki sposób dobrze sformułować **zasady zarządzania informacjami**, które będą obowiązywać nie tylko pracowników działających w trybie stacjonarnym, hybrydowym lub zdalnie, lecz także dostawców oraz kontrahentów.

Ze względu na obowiązek prawny przechowywania niektórych dokumentów i danych przez długi czas, równie ważna jest **archiwizacja informacji, zarówno tej w formie fizycznej jak i cyfrowej**. Istotne jest także wprowadzenie kompleksowego planu **użytkowania dokumentów i sprzętu IT**, które nie są już używane w organizacji.

## 3

### TWORZENIE KULTURY WSPARCIA

#### FAKTY:

50% osób odczuwało **stres z powodu błędów**, który popełniły w pracy.

#### ROZWIĄZANIE:

Udowodniono, że wprowadzenie środowiska pracy w trybie hybrydowym przyczynia się do wzrostu produktywności, jednak może ona zostać stłumiona przez stres. Należy upewnić się, że istniejący **workflow umożliwia zarządzanie ryzykiem** i rozważyć wdrożenie nowych **technologii wspieranych przez sztuczną inteligencję i uczenie maszynowe**, które pomogą **usprawnić i podnieść na wyższy poziom** procesy w organizacji.

**Co to jest budowanie „odporności” (business resilience) na etapie projektowania”?**

**Odporność** - czyli zdolność organizacji do odpierania ataków - nigdy nie powinna być traktowana drugorzędnie, lecz być nieodłącznie wpisana w każdy aspekt polityki firmy oraz procesów biznesowych.

## Integracja technologii po pandemii

Ponad połowa (59%) menedżerów danych, z którymi rozmawialiśmy, podczas pandemii **zakupiła nowe oprogramowanie**, a dwie trzecie (62%) **wdrożyło narzędzia do pracy zdalnej**, takie jak Microsoft Teams.

Należy je uwzględnić w programach zarządzania cyklem życia informacji, włącznie z **ustanowieniem okresów przechowywania danych nieustrukturyzowanych**, takich jak czaty i nagrania ze spotkań, a także z wprowadzeniem scentralizowanego systemu przestrzegania zgodności z przepisami i zarządzania polityką organizacji. To pomoże zapewnić dostosowanie się do współczesnego, coraz bardziej złożonego technologicznie środowiska pracy.

4

## EWOLUCJA PROCESÓW W ORGANIZACJI

### FAKTY:

Zdaniem 35% pracowników dane związane z ich pracą zawodową są **lepiej chronione w biurze niż w domu**.

### ROZWIĄZANIE:

Wraz z postępującą modernizacją tworzone są coraz większe ilości danych, w tym informacji wrażliwych i prywatnych. Należy zatem **przemysśleć od nowa cały proces zarządzania informacjami**: zarządzanie prawami dostępu, udostępnianie informacji cyfrowych, przechowywanie danych i zarządzanie danymi niestrukturalnymi. Pierwszym krokiem powinno być **stworzenie mapy danych**, która pozwoli zrozumieć, w jaki sposób dane napływają i wpływają z organizacji.

5

## PROWADZENIE PRAKTYCZNYCH SZKOLEŃ

### FAKTY:

Według 60% menedżerów danych, **frekwencja na szkoleniach** na temat zarządzania ryzykiem jest wysoka, natomiast 36% pracowników twierdzi, że nigdy w nich nie uczestniczyło.

### ROZWIĄZANIE:

Choć dostępne są całe moduły szkoleń na temat ryzyka, wyniki naszej ankiety wskazują, że wiedza ta szybko ulega zapomnieniu. Aby zwiększyć efektywność jej przyswajania, **szkolenia powinny być bardziej angażujące, przekazywać wiedzę, która jest bezpośrednio przydatna** i możliwa do zastosowania w praktyce. Dzięki temu pracownicy będą mogli codziennie korzystać z nabytych umiejętności, ponieważ będą lepiej rozumieć ich znaczenie w pracy własnej i z klientami.

„Wszyscy jesteśmy ludźmi i popełniamy błędy, więc ryzyko jest czynnikiem nieodłącznie związanym z pracą zawodową, jednak nie zawsze w tej samej postaci. Nowe modele biznesowe, praca hybrydowa i rosnące zagrożenie cyberatakami sprawiają, że obecnie bardziej niż kiedykolwiek istotne jest skuteczne zarządzanie ryzykiem wewnętrznym, w celu zbudowania długoterminowej odporności organizacji (business resilience).”

**Sue Trombley, Managing Director of Thought Leadership, Iron Mountain**

# "ODPORNOŚĆ NA ETAPIE PROJEKTOWANIA" (BUSINESS RESILIENCE) JAKO STAŁY ELEMENT STRATEGII

3



Według naszej ankiety, w opinii **70%** wszystkich menedżerów danych w Europie odpowiedzialność za zarządzanie ryzykiem spoczywa na wszystkich pracownikach.

„O ile element podejmowania ryzyka może przyczynić się do wprowadzania innowacji przez organizację, to jednak brak świadomości codziennych zagrożeń może osłabić jej odporność w tym zakresie. Dlatego zalecamy, aby każdy pracownik stał się ambasadorem ryzyka, co istotnie pomoże osadzić świadomość ryzyka w kulturze organizacji. Takie działanie tworzy bezpieczną przestrzeń, w której ludzie mogą wprowadzać innowacje, a organizacje rozwijać się.”

**Sue Trombley, Managing Director of Thought Leadership, Iron Mountain**

Aby odporność na ryzyko zagościła w organizacji na stałe, powinna być uwzględniana na każdym etapie tworzenia procesów biznesowych i wzmocniana poprzez działania podejmowane codziennie przez wszystkich pracowników. **To właśnie jest „odporność już na etapie projektowania”.**

Sektor publiczny prężnie pracuje nad wdrożeniem nowych technologii, takich jak sztuczna inteligencja, i odpowiada na stale rosnące zapotrzebowanie na dostęp mobilny i komunikację między departamentami. Dlatego ważne jest, aby zdać sobie sprawę, że podwyższone zagrożenie cyberatakami prawdopodobnie utrzyma się, gdy powrócimy do normalności po pandemii COVID-19.

W związku z tym **wdrożenie „odporności na etapie projektowania” w rozwiązaniach opartych na pracy hybrydowej** ma kluczowe

znaczenie dla długoterminowego powodzenia każdej organizacji sektora publicznego. Są to na przykład rozwiązania zapewniające [bezpieczny dostęp do informacji](#) dla pracowników czy obywateli z dowolnego miejsca na świecie, [usprawniające codzienną pracę](#) oraz pomagające skutecznie zarządzać całym cyklem życia danych, niezależnie od ich formatu i rodzaju. Istotne jest przy tym, aby przyjęte rozwiązania generowały dodatkową wartość dla organizacji i dla społeczeństwa.

Aby uzyskać wsparcie w stawianiu czoła wciąż ewoluującym wyzwaniom w zakresie zarządzania informacjami w Twojej organizacji i omówić rozwiązania, które pomogą Ci zwiększyć jej odporność w świecie pracy hybrydowej, zapraszamy do kontaktu lub odwiedzenia strony [ironmountain.com/pl](https://ironmountain.com/pl)

## O IRON MOUNTAIN

Firma Iron Mountain Incorporated (NYSE: IRM) powstała w 1951 roku i jest światowym liderem w dziedzinie usług magazynowania i zarządzania informacjami. Cieszy się zaufaniem ponad 220000 organizacji na całym świecie, posiadająca sieć nieruchomości obejmującą prawie 8 milionów metrów kwadratowych, w ponad 1400 obiektach, w 50 krajach, firma Iron Mountain przechowuje i chroni cenne zasoby, w tym krytyczne informacje biznesowe, wrażliwe dane oraz artefakty kulturowe i historyczne. Zapewnia rozwiązania obejmujące bezpieczne przechowywanie, zarządzanie informacjami, transformację cyfrową, bezpieczne niszczenie, a także centra danych, przechowywanie dzieł sztuki i logistykę oraz usługi w chmurze. Firma Iron Mountain pomaga organizacjom obniżyć koszty i ryzyko, zapewnić zgodność z przepisami prawa, przywrócić działalność w przypadku wystąpienia katastrofy i umożliwić bardziej cyfrowy sposób pracy. Aby uzyskać więcej informacji, odwiedź stronę [www.ironmountain.pl](http://www.ironmountain.pl).

© 2021 Iron Mountain Incorporated. Wszelkie prawa zastrzeżone. Iron Mountain i wizerunek góry są zarejestrowanymi znakami towarowymi firmy Iron Mountain Incorporated w Stanach Zjednoczonych i innych krajach. Wszystkie inne znaki towarowe są własnością ich właścicieli.

801800802 | [IRONMOUNTAIN.COM/PL](http://IRONMOUNTAIN.COM/PL)

