



**DOBRE PRAKTYKI: PRZEWODNIK DLA
SEKTORA OPIEKI ZDROWOTNEJ**

MIARĄ SIŁY ORGANIZACJI JEST WYTRZYMAŁOŚĆ JEJ NAJSŁABSZEGO OGNIWA

**Jak uwzględniać 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).

Nigdzie problem ten nie jest bardziej widoczny niż w sektorze ochrony zdrowia, w którym coraz bardziej wyrafinowane cyberataki stanowią zagrożenie dla poufnych danych pacjentów. Tymczasem, podatność na atak rośnie w miarę migracji kartotek medycznych do platform cyfrowych, coraz częstszego udzielania porad zdalnie i wykorzystania urządzeń IoT. Zapewnienie efektywnej, zdalnej obsługi pacjentów, przy zachowaniu bezpieczeństwa ich informacji, w sposób zgodny z przepisami, nigdy nie było bardziej istotne.

CZY WIESZ, ŻE?

W maju 2021 r. irlandzki system ochrony zdrowia doświadczył ataku ransomware, tj., oprogramowania przechwytyującego dane w celu wymuszenia okupu, w rezultacie większość szpitali w Irlandii nie mogła korzystać z komputerów przez **ponad tydzień**¹.

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 błędy ludzkie, mogą być one niezwykle kosztowne stwarzając zagrożenie dla życia pacjentów, powodując straty finansowe, nie wspominając o uszczerbku na reputacji, w przypadku gdy dochodzi do utraty wrażliwych informacji medycznych.

W raporcie przygotowanym niedawno przez IBM średni koszt jednego naruszenia ochrony danych dotyczących zdrowia oszacowano na **9,23 mln USD** - więcej niż w jakiegokolwiek innej branży².

Z tego względu Iron Mountain zlecił przeprowadzenie ogółouropejskiego badania³ 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.

ROZDZIAŁY W PRZEWODNIKU

1. 10 dni po ataku ransomware system opieki zdrowotnej w Irlandii wciąż borykał się z problemami.

2. Przygotowany przez IBM raport pt. „Koszty naruszenia ochrony danych” (Cost of a Data Breach), 2020 r.

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

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

BUDOWANIE ŚWIADOMEJ RYZYKA KULTURY ORGANIZACYJNEJ

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 **popętnienia „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 ochrony zdrowia wdrożyły mechanizmy awaryjnego reagowania, które obecnie zostały przekształcone w długoterminowe strategie zbudowane wokół zdalnych konsultacji i pracy hybrydowej. Należy się zastanowić, w jaki sposób dobrze sformułować **zasady zarządzania informacjami**, które będą obowiązywać nie tylko pracowników, lecz także dostawców oraz kontrahentów.

W miarę przyspieszania procesów cyfryzacji kartotek pacjentów, krytycznego znaczenia nabiera zapewnienie **łańcucha nadzoru (chain of custody)** w ramach procesów gromadzenia, przesyłania, digitalizowania i usuwania danych.

3

TWORZENIE KULTURY WSPARCIA

FAKTY:

50% osób odczuwało **stres z powodu błędu**, 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. Biorąc pod uwagę rosnącą liczbę danych, należy się upewnić, że **struktura workflow umożliwia zarządzanie ryzykiem** i jest dobrze dostosowana do systemów zawierających coraz bardziej kompleksowe informacje. Warto rozważyć wdrożenie skalowalnych, nowych **technologii wspieranych przez sztuczną inteligencję i uczenie maszynowe**. Pomagają one w **usprawnieniu procesów i powodują podniesienie ich na wyższy poziom**, dzięki czemu Twoi pracownicy będą mogli skoncentrować się na tym, aby świadczone przez nich usługi opieki zdrowotnej były jak najwyższej jakości i aby możliwie jak najszybciej przyjąć wszystkich oczekujących w kolejkach powstałych na skutek pandemii.

Co to jest budowanie „odporność” (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 z pacjentami i nagrania zdalnych konsultacji, 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:

Zdalne porady i wprowadzenie cyfrowych szpitalnych kartotek pacjentów, które szybko stały się normą, generują coraz większe ilości danych. W tej sytuacji należy **przemyśleć od nowa cały proces zarządzania informacjami**: zarządzanie prawami dostępu, udostępnianie informacji cyfrowych, przechowywanie danych i zarządzanie danymi nieustrukturalnymi. 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 dla swoich pacjentów.

„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

BUDOWANIE ŚWIADOMEJ RYZYKA KULTURY ORGANIZACYJNEJ

2

"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 ona uwzględniana już na etapie projektowania, a także na każdym etapie tworzenia procesów biznesowych i wzmacniana poprzez działania podejmowane codziennie przez wszystkich pracowników, zarówno klinicznych jak i administracyjnych.

Obecnie dostawcy usług ochrony zdrowia pracują nad szybkim zdigitalizowaniem swoich procesów operacyjnych. W kontekście uderzenia pandemii COVID-19, po którym wciąż dochodzimy do siebie, uświadomienie sobie, że zwiększone zagrożenie cyberatakami prawdopodobnie pozostanie z nami na zawsze, jest niezwykle istotne.

W związku z tym **wdrożenie „odporności na etapie projektowania” w rozwiązaniach opartych na pracy hybrydowej** ma kluczowe znaczenie dla długoterminowego powodzenia każdej organizacji świadczącej usługi ochrony

zdrowia. Są to na przykład rozwiązania zapewniające [bezpieczny dostęp do informacji](#) z dowolnego miejsca na świecie, [usprawniające przepływy pracy](#) związane z archiwizacją i digitalizowaniem kartotek i rejestrów, a także pomagające skutecznie zarządzać całym cyklem życia danych pacjenta, niezależnie od ich formatu i rodzaju. Istotne jest przy tym, aby przyjęte rozwiązania chroniły i ulepszały dostępność informacji w Twojej klinice, a zarazem usprawniały proces podejmowania decyzji i podnosiły jakość opieki nad pacjentem.

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/industries/healthcare-services.

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.

© 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

