IRON MOUNTAIN®

DOBRE PRAKTYKI: PRZEWODNIK DLA SEKTORA FINANSOWEGO

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 usług finansowych, w którym zarządzanie ryzykiem ma zasadnicze znaczenie dla codziennych operacji i przesądza o przewadze konkurencyjnej. Należy też pamiętać, że podatność na zagrożenia rośnie wraz z rozwojem nowych modeli biznesowych - od kryptowalut po otwartą bankowość i płatności online.

CZY WIESZ, ŻE?

Na podstawie informacji dostępnych w rejestrze przestępstw popełnionych w okresie pandemii COVID-19 (Covid Crime Index) prowadzonym przez BAE Systems, **trzy czwarte (74%)** banków i towarzystw ubezpieczeniowych doświadczyło **wzrostu cyberprzestępczości** w okresie pandemii, a **42% z nich stwierdziło, że praca w trybie zdalnym przyczyniła się do pogorszenia ich bezpieczeństwa**.

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. Skutki takich zachowań są najbardziej dotkliwe właśnie w sektorze usług finansowych.

W niedawno ogłoszonym raporcie przygotowanym przez IBM średni koszt naruszenia ochrony danych oszacowano na **4,24 mln USD**[1].

Z tego względu Iron Mountain zlecił przeprowadzenie ogólnoeuropejskiego badania[2] wskazującego na potencjalne obszary, gdzie ludzkie słabości stanowią kluczowy czynnik w zarządzaniu ryzykiem w organizacji. Wyniki okazały się zaskakujące.

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

1. Przygotowany przez IBM raport pt. „Koszty naruszenia ochrony danych" (Cost of a Data Breach), 2021 r.
2. Badanie 11 000 pracowników w 10 krajach, przeprowadzone we wrześniu 2021 r. przez One Poll.

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?

KLIKNIJ NA IKONY I DOWIEDZ SIĘ WIĘCEJ!

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 **popełnienia „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 PODCZAS **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 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 **utylizacji dokumentów i sprzętu IT**, które nie są już używane w organizacji.

3 TWORZENIE KULTURY WSPARCIA

FAKTY:

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

ROZWIĄZANIE:

Udowodniono, że wprawdzie środowisko 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 takie jak analizowanie wniosków o kredyty hipoteczne i pożyczki gotówkowe.

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.

BUDOWANIE ŚWIADOMEJ RYZYKA KULTURY ORGANIZACYJNEJ

2

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:

Otwarta bankowość i wprowadzenie płatności cyfrowych, 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 niestrukturalnymi. Pierwszym krokiem powinno być **stworzenie mapy danych**, która pozwoli zrozumieć, w jaki sposób dane napływają i wypływają 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:

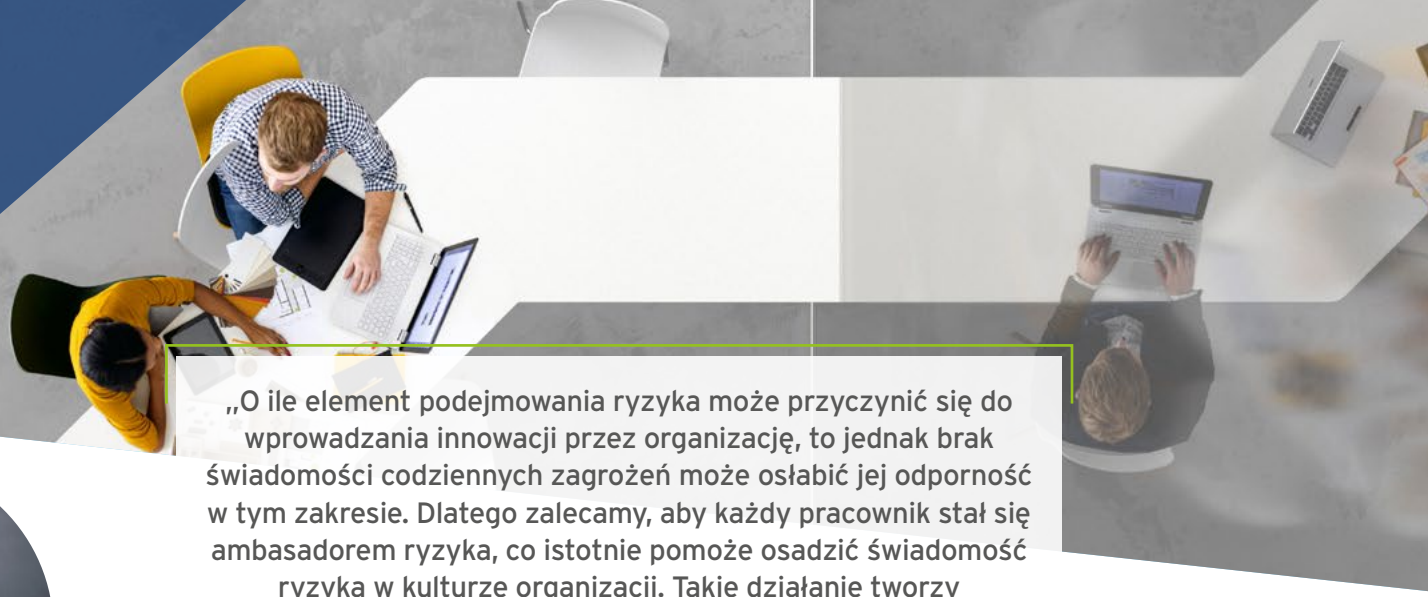
Choć dostępne są całe moduły szkoleń na temat ryzyka, wyniki naszej ankiety wskazują, że wiedza ta szybko ulega zapomnieniu. Aby zwiększyć efektywność jej przyswajania, **szkolenia powinny być bardziej angażujące, przekazywać wiedzę, która jest bezpośrednio przydatna** i możliwa do zastosowania w praktyce. 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



„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

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

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

Obecnie dostawcy usług finansowych opracowują swoje strategie długoterminowe od nowa. W kontekście uderzenia pandemii COVID-19, po którym wciąż dochodzimy do siebie, uświadomienie sobie, że ryzyko nieoczekiwanych zmian na rynku 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 finansowe. Są to na przykład rozwiązania zapewniające bezpieczny dostęp do informacji z dowolnego miejsca na świecie, usprawniające workflow przy przetwarzaniu wniosków o kredyty hipoteczne i pożyczki gotówkowe 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.

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/financial-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.

801800802 | IRONMOUNTAIN.COM/PL

IRON MOUNTAIN®