Zarządzanie ryzykiem

– Święty Graal czy wielka mistyfikacja?

Żaden dyrygent nie powie, że ma najlepszych instrumentalistów i oni najlepiej będą wiedzieli, jak grać (przecież przygotował partyturę, a każdy muzyk ma swoje nuty), a on im nie będzie przeszkadzał. A niestety, tak działa wiele organizacji w sferze cyberbezpieczeństwa, tylko tam rolę partytury i nut pełnią dokumenty polityk, procedur i instrukcji.

Paweł Henig

absolwent Wydziału Elektroniki Politechniki Warszawskiej. Od połowy lat 90. budował dla centralnej administracji rządowej centra przetwarzania danych i sieci rozległe. Audytor wewnętrzny systemów zarządzania obejmujących normy: zarządzania jakością (ISO 9001), zarządzania środowiskowego (ISO 14001), zarządzania bezpieczeństwem i higieną pracy (OHSAS 18001), bezpieczeństwem produkcji wartościowej (CWA 14641 – Intergraf) oraz zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001. Certyfikowany audytor systemów IT (CISA), posiadacz certyfikatu ITIL Foundation. Rzeczoznawca PTI, ekspert PIIT. Dyrektor Operacyjny Trusted Information Consulting Sp. z o.o.

Podejście bazujące na ryzyku (ang. *risk-based approach*) jest obecnie kojarzone z nowoczesnymi metodami zarządzania. Ugruntowało ono swoją pozycję w świecie finansów, kojarząc się najczęściej z obszarem ubezpieczeń albo kredytów. Praktycznie każdy w swoim życiu spotkał się z określeniem „ryzyko ubezpieczeniowe" czy „ryzyko kredytowe", pojęcia te rozumiemy niejako intuicyjnie. Znacznie gorzej będziemy rozumieli kwestię ryzyka np. w przypadku przeciwdziałania praniu „brudnych" pieniędzy (ang. *Anti-Money Laundering – AML*), które jest wymogiem prawnym między innymi w Polsce. No cóż, nie każdy musi być specjalistą od sposobów działania zorganizowanej przestępczości (w tym związanej z terroryzmem), a w szczególności – wykorzystania przez nią legalnego obrotu prawnego celem uwiarygodnienia dochodów pochodzących z nielegalnej działalności.

Ryzyko jest związane z niepewnością. Odnosi się do przyszłych skutków w odniesieniu do podjętych działań lub zaniechań. De facto każde nasze działanie, a w szczególności podejmowane przez nas decyzje, wynikają z podejścia opartego na ryzyku. Zarządzamy ryzykiem planując spacer, bo sprawdzamy pogodę, aby odpowiednio się ubrać oraz ewentualnie zabrać ze sobą parasol. Zarządzamy ryzykiem wybierając drogę do pracy, powrót do domu, wyjazd na wakacje czy przechodząc przez ulicę. Często robimy to intuicyjnie. Wiele z podejmowanych przez nas decyzji wynika z doświadczenia lub wyrobionych nawyków (np. edukacja dzieci na temat zachowania w ruchu miejskim czy kontaktów międzyludzkich). Niezbędna jak również umiejętność pozyskiwania informacji (np. prognozy pogody).

Kierownictwu z ryzykiem nie po drodze

Skoro kwestie ryzyka nie są nam obce, to dlaczego sprawia ono tyle problemów w ochronie danych osobowych czy bezpieczeństwie informacji (cyberbezpieczeństwie)? Dlaczego w trakcie audytu tak trudno uzyskać konkretne, merytoryczne odpowiedzi, ale za to często można spotkać się z poniższymi stwierdzeniami mającymi na celu usprawiedliwienie, a właściwie zakwestionowanie dokonanych spostrzeżeń?

> „Analiza ryzyka to bardziej sztuka niż nauka" – pytanie: czy z wyboru, czy zgodnie z projektem?
>
> „Pracuje u nas nad tym grupa najlepszych ekspertów" – w domyśle „to jest zadanie dla specjalistów, nie dla kierownictwa".
>
> „Zadanie jest bardzo skomplikowane, tego nie da się tak prosto wytłumaczyć! W rejestrze mamy kilka tysięcy ryzyk!" – w domyśle „bardzo się nad tym napracowaliśmy, miało być więc jest" – vs. „od tego mam ludzi i nie muszę się na tym znać"
>
> „Wszystko jest opanowane: 90% ryzyk jest „na zielono", pozostałe 10% „na żółto", wszystko na bieżąco monitorujemy".
>
> „Inni audytorzy chwalili naszą analizę, a nie szukali dziury w całym".

Niestety, podstawowa przyczyna takiego stanu związana jest z postawą kierownictwa badanej jednostki. Wszystkie systemy zarządzania bazujące na normach zharmonizowanych funkcjonujących w systemie prawnym Unii Europejskiej wymagają „przywództwa i zaangażowania". I nie chodzi tu o frazeologiczną deklarację, lecz o ściśle określone działania, w szczególności w zakresie:

- ustanowienia celów zgodnych z kierunkiem strategicznym organizacji;
- zintegrowania wymagań systemu zarządzania z funkcjonowaniem organizacji;
- zapewnienia dostępności potrzebnych zasobów;
- zapewnienia, że system zarządzania osiąga zamierzone wyniki (mierniki osiągnięcia celów, skuteczność);
- kierowanie i wspieranie osób przyczyniających się do osiągnięcia skuteczności odpowiednio do obszarów ich odpowiedzialności.

Zarządzający musi być zatem liderem integrującym zespół, a nie szefem działającym zgodnie z łacińską maksymą *divide et impera*[1]. Lider nie musi „znać się na wszystkim", tak jak dyrygent nie musi być wirtuozem wszystkich instrumentów w orkiestrze symfonicznej. Lider musi działać tak jak dyrygent. Musi nadawać kierunek (dysponując niezbędnym zespołem i znając jego ograniczenia), jak również musi korygować pojawiające się zakłócenia lub niedociągnięcia tak, aby wykonać swoje zadanie jak najlepiej.

No dobrze, powie ktoś, ale tam nie ma słowa o ryzyku. Czy na pewno?

Definicja ryzyka

Ogólna definicja zawarta w ISO Guide 73 oraz w normie ISO 31000 definiuje ryzyko jako „wpływ niepewności na cele". Norma ISO/IEC 29100 odnosząca się do ochrony danych osobowych określa ryzyko[2] (dokładniej *privacy risk*)

1 Dziel i rządź – starorzymska zasada waśnienia innych, by łatwiej nimi rządzić.

2 Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO) nie zawiera definicji ryzyka.

jako „wpływ niepewności na prywatność". Norma ISO/IEC 27005 wprowadza ryzyko związane z bezpieczeństwem informacji, które określa: „potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę dla organizacji". Norma ta zawiera dodatkowe wyjaśnienie, uwagę informującą, iż „ryzyko jest mierzone jako kombinacja prawdopodobieństwa zdarzenia i jego następstw". Natomiast zgodnie z Dyrektywą NIS, ryzyko oznacza „każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych".

Niestety, ustawa o krajowym systemie cyberbezpieczeństwa (KSC) implementująca Dyrektywę NIS w polskim porządku prawnym błędnie definiuje ryzyko, gdyż podaje definicję miary ryzyka („kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji") zamiast definicji, czym jest ryzyko. Są to dwa różne pojęcia, czego ewidentnie nie dostrzega lub nie rozumie ustawodawca, a w ślad za tym regularnie powielane są błędy wdrożeniowe, w szczególności w przypadku literalnego interpretowania wymagań lub opierania się „wyłącznie na wymaganiach prawnych".

Zrozumienie sensu ryzyka wymaga powrotu do źródła, czyli zrozumienia celów. Tym celem w przypadku ochrony danych osobowych jest zapewnienie prywatności, natomiast w przypadku bezpieczeństwa informacji jest ochrona wartości (aktywa, czyli zgodnie z definicją zawartą w normach z serii ISO/IEC 27000, wszystko co ma wartość), innymi słowy zapobieganie szkodzie. W przypadku systemu zarządzania bezpieczeństwem informacji mówi się o celach w odniesieniu do cech, własności informacji[3], których utrata może tę szkodę powodować. Natomiast przytoczona powyżej definicja odniesiona do bezpieczeństwa informacji (cyberbezpieczeństwa) ma charakter przyczynowo-skutkowy (okoliczność lub zdarzenie mogące mieć niekorzystny wpływ, powodujące szkodę) i stanowi niejako uzupełnienie definicji ogólnej (wpływ niepewności na cele). Skoro zatem ryzyko łączy się bezpośrednio z celami oraz ich osiąganiem (między innymi poprzez właściwe oszacowanie niezbędnych zasobów, również osobowych), to znaczy, że „podejście oparte na ryzyku" jest podstawowym sposobem wykazywania „przywództwa i zaangażowania" przez najwyższe kierownictwo.

> *„Podejście bazujące na ryzyku jest spoiwem działań zarządczych, a od jakości, dokładności i czytelności informacji o ryzyku zależy trafność podejmowanych decyzji, a tym samym skuteczność całego systemu zarządzania. System zarządzania nie powinien się opierać wyłącznie na intuicji.*

Niestety, najczęściej nikt nie uświadamiał tego kierownictwu, a konieczność „posiadania analizy ryzyka" została przedstawiona jako „dopust boży" lub „biurokratyczny wymysł". Idąc po linii najmniejszego oporu, skoro coś trzeba posiadać, to znaczy należy to kupić, tak jak cukier czy jabłka, które trzeba mieć, mimo że nikt nie słodzi ani nie lubi jabłek.

Wtedy często do gry wchodzi „najniższa cena" lub inna forma „szybkiego zlecenia", bo przecież „liczy się sztuka". Zamawiamy zatem „dokument analizy ryzyka zgodny z czymś tam" (da się znaleźć w Internecie podobne zamówienie i magiczną metodą kopiuj-wklej mamy gotowe zamówienie). Jak krótkowzroczne jest to podejście, przekonał się wójt gminy Dobrzyniewo Duże, któremu UODO nałożył administracyjną karę pieniężną w listopadzie 2022 r. za niezapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz brak wdrożenia odpowiednich środków technicznych i organizacyjnych ujętych w analizie ryzyka (źródło https://uodo.gov.pl/pl/138/2493). Czy zdarzenie to coś zmieni w podejściu do analizy ryzyka w zarządzaniu bezpieczeństwem informacji? Chciałbym w to wierzyć. Niestety, nadal największym problemem będzie pozyskanie rzetelnego wsparcia z rynku, na którym dominują dostawcy „gotowych dokumentów" dostępnych po „najniższej cenie", gdyż sprzedając wielokrotnie ten sam towar różnym klientom mogą sobie pozwolić na taki komfort. Fakt, że jest to działanie nieetyczne wielu osób nie interesuje, gdyż po prostu dostarczają to, co klient chce kupić. Ostatecznie „mamy wolny rynek" – argumentują.

Podstawowym problemem jest zatem uświadomienie kierownictwu:

- czego faktycznie potrzebuje;
- co będzie stanowiło dla niego faktyczną wartość;

3 W przypadku bezpieczeństwa informacji, tymi podstawowymi cechami są: poufność, integralność oraz dostępność.

- co pomoże mu w podejmowaniu racjonalnych decyzji i uchroni przed popełnieniem błędu, a jeśli już się wydarzy, to pozwoli wykazać zachowanie należytej staranności.

Dziś analiza ryzyka w bezpieczeństwie informacji (cyberbezpieczeństwie) jest znacznie częściej wielką mistyfikacją niż Świętym Graalem.

Najczęściej popełniane błędy *by design*[4]:

- Zarządzanie ryzykiem nie jest zintegrowane ze wszystkimi przedsięwzięciami i działaniami. Zazwyczaj są to światy „równoległe". Jest bieżące zarządzanie oraz najczęściej sformalizowane zarządzanie ryzykiem czy inne działania „systemowe" stanowiące odrębny wątek (zwykle przeszkadzający w rutynowym działaniu).
- Zarządzanie ryzykiem nie jest ustrukturyzowane i kompleksowe, gdyż nie angażuje zasobów na wszystkich poziomach organizacyjnych, a role i odpowiedzialności w zakresie zarządzania ryzykiem są przypisane do pojedynczych osób, które zazwyczaj nie posiadają kompleksowej wiedzy, jak również uprawnień do zaangażowania osób, które tą wiedzą dysponują.
- Zarządzanie ryzykiem nie jest dostosowane do kontekstu i celów organizacji. Najczęściej stosowany jest jeden szablon dostarczony przez konsultanta wraz z „wykonaną analizą ryzyka". Wymaga się od konsultanta „jako wybitnego specjalisty", aby zrobił to samodzielnie, nie angażując zasobów organizacji, która ma inne, ważniejsze zadania.
- Zarządzanie ryzykiem nie jest inkluzywne (niewykluczające), czyli nie angażuje wszystkich zainteresowanych stron. Często organizacje nawet nie zidentyfikowały wszystkich stron zainteresowanych zarządzaniem ryzykiem.
- Zarządzanie ryzykiem nie ma charakteru proaktywnego, szybko reagującego, przewidującego zmiany otoczenia. Zazwyczaj zarządzanie ryzykiem wykonywane jest raz do roku albo po wystąpieniu jakiegoś poważnego incydentu, czyli ma charakter całkowicie reaktywny.
- Zarządzanie ryzykiem nie korzysta z najlepszych dostępnych informacji. Często bazuje na odczuciach lub służy celom uzasadnienia podjętych decyzji (ex post). Sprzyja temu powszechnie stosowana tzw. mapa ciepła (ang. *heat map*), która nie uwzględnia teorii rachunku prawdopodobieństwa ani tolerancji, oceny jakości posiadanych informacji, a samo oszacowanie jest deterministyczne, chociaż powinno odnosić się do przyszłości (czyli powinno uwzględniać niepewność).
- Zarządzanie ryzykiem nie uwzględnia czynników ludzkich i kulturowych. Zupełnie inaczej powinno się komunikować z zarządem, a zupełnie inaczej z ekspertami dziedzinowymi w zakresie np. sieci komputerowych czy architektury systemów. Nic dziwnego, że nie dostrzegając użyteczności informacji związanych z zarządzaniem ryzykiem, traktują oni tę aktywność jako niepotrzebną stratę czasu.
- Zarządzanie ryzykiem nie uwzględnia ciągłego doskonalenia. Zazwyczaj jest działaniem rutynowym, niepowiązanym z żadnymi miernikami, które pozwoliłyby na podejmowanie decyzji doskonalących. Co najwyżej mówi się o terminowości, ale jedynie w kontekście niezgodności (nieterminowego wykonania analiz).

[4] Dosłownie poprzez projekt, w sposób zamierzony, intencyjnie. Pojęcie wprowadzone w motywie 78, 108 i artykule 25 RODO, które lepiej oddaje sens regulacji i jest stosowane równolegle do polskiego tłumaczenia „uwzględniania w fazie projektowania".