

## *XIV Międzynarodowy Kongres Kontroli, Audytu, Antykorupcji i Zwalczania Oszustw*

URSZULA KAMIŃSKA



Międzynarodowy Kongres Kontroli, Audytu, Antykorupcji i Zwalczania Oszustw to niewątpliwie najważniejsza w roku impreza dla środowiska kontrolerskiego. Ma już czternastoletnią tradycję, ogromne perspektywy na przyszłość i jubileuszową edycję już za 9 miesięcy.

**C**o roku we wrześniu w Krakowie eksperci, specjaliści i praktycy audytu, kontroli, antyfraudu i antykorupcji z całego świata spotykają się na Międzynarodowym Kongresie, by wymienić się doświadczeniami, informacjami o najnowszych regulacjach w przedmiotowym zakresie, zaprezentować rozwiązania, które stosują w swoich organizacjach, omówić systemy, modele, narzędzia i metody pozwalające pokonywać problemy, z jakimi na co dzień muszą się mierzyć.

Głównym przedmiotem zainteresowania XIV Kongresu, który obradował 24 i 25 września 2015 roku, były narzędzia i strategię aktywnej obrony przed nadużyciami, oszustwami i korupcją. Temat interesujący i ciągle palący, nic więc dziwnego, że wzbudził zainteresowanie nie tylko uczestników i gości imprezy, ale także mediów, zawodowych stowarzyszeń kontrolerskich, organizacji sektora publicznego i prywatnego, dla których fraudy i korupcja to codzienne zmartwienie i wyzwanie. Ważka idea Kongresu okazała się także inspiracją dla uczest-

ników spotkania, jeden z nich zamierza zorganizować podobną konferencję w Baku, drugi przysłał propozycję uatrakcyjnienia przyszłych Kongresów.

W większości wystąpień podkreślano kluczową rolę zarządzania ryzykiem w obronie przed zawnionymi, celowymi i przypadkowymi stratami przedsiębiorstwa. Podkreślano, jak trudno niejednokrotnie zidentyfikować zagrożenia, bo oszuści są bardziej kreatywni niż wielu z nas przypuszcza. Pokazano, jak bardzo potrzebna jest ostrożność w korzystaniu z nowinek technicznych i nowoczesnych technologii, którymi oszuści często sprawniej operują niż specjaliści zatrudniani przez organizacje. Ale jak sprawnie zarządzać ryzykiem oszustwa, kiedy zdecydowana większość klientów, pracowników i kandydatów do pracy nie mówi prawdy o sobie, zdecydowana większość firm w większym lub mniejszym stopniu manipuluje swoim bilansem oraz danymi o dochodach i zyskach, a większość osób i firm, wykorzystuje istniejące luki prawne oraz niekompetencję urzędników i kontrolerów do swoich celów. Mała szansa, że się to uda, jeśli właściciele firm i ich kierownicy nie będą dokładnie przyglądać się kandydatom do pracy.

Według różnych badań, średnio w 94% przedsiębiorstwach występują większe lub mniejsze nadużycia, a w ich wyniku, w zależności od branży, straty wahają się od 3 do 30% dochodów. Sprawcy nadużyć w polskich przedsiębiorstwach to głównie osoby skupiające pełnię władzy w firmie lub posiadające olbrzymi wpływ na to, co się w niej dzieje. Wśród dużej grupy młodszych oszustów znajdują się osoby pełniące funkcje kierownicze w departamentach sprzedaży/marketingu oraz zakupów, inaczej niż na świecie, gdzie prym wiodą pracownicy działów finansowych.

Z codziennego życia wiemy, że człowiek na miejscu kłopoty. Kiedy zatrudniony jest lub znając



jego d z a  
jętności nie  
by sprostać obo-  
wianym do zajmowanego stanowiska, po prostu nie powierza mu się zadań, przez które mogłyby powstać straty. Inaczej mają się sprawy, gdy w firmie pojawi się oszust kompetencyjny, którego portret został w jednej z prelekcji dobrze nakreślony. Nie jest łatwo go zidentyfikować, bo z założenia potrafi się skutecznie maskować, zmieniać obszar działania, a oszukiwać może zarówno w składanej dokumentacji (sfabrykowane życiorysy, listy polecające, świadectwa, itp.), jak i prezentowanej postawie wobec firmy i jej pracowników i zawsze dopasowuje prezentowany wizerunek do sprawnie rozpoznanych potrzeb i oczekiwań organizacji. Zdarza się, że czyny oszustów kompetencyjnych nie spełniają kryteriów przestępstwa, ale nawet wtedy powodują u innych ogromne koszty osobiste, firma zaś ponosi ekonomiczne, psychologiczne, społeczne, fizyczne straty. Największy problem kompetencyjnego oszustwa to menedżerowie wysokiego i najwyższego szczebla, dlatego, że działania szefów – ich zaburzenia stają się zaburzeniami całej organizacji. Dlatego właściciele szczególnie dokładnie powinni przyglądać się osobom, którym powierzają swój kapitał w zarząd.

W wielu organizacjach czas jakby się zatrzymał. System oparty na badaniach ryzyka z okresu założycielskiego, skonstruowany według norm i wymogów np. sprzed ćwierćwiecza nie jest w stanie poradzić sobie z dzisiejszymi zagrożeniami. Zarządzanie organizacją bez uświadomienia sobie, że audyt dzisiaj, to nie to samo co audyt 25 lat temu, oczekiwanych efektów nie



## WAŻNE WYDARZENIE

przyniesie, jeśli nie będzie nadążać za zmieniającą się rzeczywistością.

Każda firma, korporacja, jednostka budżetowa stara się systemowo zapobiegać nadużyciom finansowym. Wprowadzając mechanizmy kontrolne, musi je permanentnie doskonalić, bowiem ludzka kreatywność nie ma granic. Ale to nie zawsze mało sprawny system, niedoskonałe procedury czy jakość działania pracowników odpowiadają za finansowe straty organizacji. Czasem winę za straty ponosi wadliwy system prawny. Ponadprzeciętna dynamika zmian prawa, jego nieprecyzyjność, która nie pozwala go po prostu stosować, bo niejednokrotnie podlega uznaniowej interpretacji urzędniczej, jego niespójność i poważne luki bywają przyczyną strat trudnych, a czasem niemożliwych do przewidzenia. Tam, gdzie prawo zawodzi, tam zdrowy rozsądek jest jedynym ratunkiem. Dokładne czytanie umów, szczególnie kredytowych, jest bardzo istotnym elementem kontrolowania ryzyka. Banki zawsze sobie poradzą, ale klient, który podpisał niekorzystną dla siebie umowę, już niekoniecznie. Wygodna płatność kartą może sporo kosztować, a niestarannie wycenione nabyte wyposażenie i środki trwałe firmy to nie większe koszty, ale realne straty.

Rzadko w Polsce wykorzystywany compliance, w USA czy Europie Zachodniej przynosi bardzo konkretne efekty, o czym zapewnili przedstawiciele dużych zagranicznych organizacji. Czytelne zasady postępowania i procedury odpowiadające konkretnym warunkom działalności, obowiązujące cały personel skutecznie



ograniczyć ryzyko i korupcji.

czają nadużyć

Dzięki jasnemu

komunikowaniu o obowiązujących zasadach przeciwdziałania fraudom i korupcji, compliance uświadamia zarówno pracowników wszystkich szczebli przedsiębiorstwa jak i podmioty trzecie z nim współpracujące o konsekwencjach ich nieprzestrzegania. System konsekwentnie stosowanych, proporcjonalnych w stosunku do naruszeń środków dyscyplinarnych oraz wymierne rozwiązania motywujące do przestrzegania programu compliance sprawdziły się na Zachodzie jako najlepsza motywacja do postępowania zgodnie z normami. Istotne jest, by program compliance pozwalał każdemu, z zachowaniem poufności i bez obawy o negatywne konsekwencje na zgłaszanie naruszeń oraz podejrzeń o nieprzestrzeganie obowiązujących zasad postępowania oraz, by procedury pozwalały na skuteczne sprawdzenie każdego takiego zgłoszenia. Uchroni to przedsiębiorstwo nie tylko przed stratami finansowymi, ale i wizerunkowymi, których koszty są ogromne, gdy do firmy wkracza prokuratura lub służby specjalne. Stała ocena przystawalności programu compliance do zmieniającego się ryzyka i wykrytych słabości programu oraz wprowadzanie stosownych zmian, zapobiegnie lub szybko pozwoli wykryć naruszenia prawa czy wewnętrznych regulacji.

Istotny i cenny dla programu compliance element – sygnalista jest jednak trudny do zrealizowania w Polsce. Nadal trudno jest przekonać zarówno pracodawców jak i pracowników, że nie jest on donosicielem, lecz osobą identyfikującą się z firmą, dbającą o jej dobro, a jednocześnie najtańszym źródłem informacji o nieprawidłowościach w firmie. Ostatnie badanie przeprowadzone przez CBOS pod kątem postrzegania i przewidywanych reakcji pracodawcy i współpracowników na sygnalistę





prokurator, choć sto- zuje, że sunek do takiej postawy złagodniał, ciągle jeszcze stanowi istotną przeszkodę, by osoba, na oczach której łamane są reguły, zasady czy przepisy prawa poinformowała przełożonego czy osobę uprawnioną przez firmę do przyjmowania takich zawiadomień. Niewątpliwie niedociągnięcia legislacyjne w tym zakresie potęgują niechęć do dzielenia się wiedzą o firmowych oszustwach czy łapownikach.

Walka z nadużyciami i korupcją nie jest prosta, tym bardziej, że służby powołane do jej zwalczania same, jak się okazuje, od takich procederów nie są wolne. Medialna wrzawa towarzysząca korupcji w publicznych urzędach, agendach rządowych czy spółkach Skarbu Państwa niestety nie działa odstrasżająco. Często wydzwięk spektakularnych akcji policji, prokuratury czy służb specjalnych przynosi efekt odwrotny. Polskie prawo nie nadąża za pomysłowością defraudantów czy łapowników, ale ostatnio pojawiły się nowe regulacje prawne w walce z nadużyciami i korupcją, które na Kongresie zostały przedstawione.

Walka ze zorganizowaną przestępczością stanowi ogromne wyzwanie nie tylko dla organów ścigania, ale i przedsiębiorstw. Nieświadomie zawierane kontrakty z firmami czy osobami należącymi do grup przestępczych mogą spowodzić podejrzenia o udział w nielegalnym procederze. Śledztwo, zatrzymanie dóbr, kontrola i przeszukania nie dość, że dezorganizują pracę, to i nie są najlepszym PR dla przedsiębiorstwa. Jeżeli organizacja dysponuje odpowiednimi mechanizmami kontrolnymi, już na etapie wyboru dostawcy czy partnera może zidentyfikować i odrzucić podejrzaną ofertę. Sprawny audyt wewnętrzny może pomóc w wykryciu nieprawidłowości w transakcjach i ich charakteru, nawet jeśli kontrahent pomyślnie przeszedł weryfikację.

Wysokie podatki i ich zróżnicowane stawki stanowią przedmiot zmyślnej spekulacji organizatorów grup przestępczych. Dochody ze sprzedaży nielegalnie spro-

wadzonych czy wyprodukowanych towarów: alkoholu, papierosów czy paliw to tylko część przestępczości podatkowej. Najbardziej lukratywny dochód stanowią wyłudzenia podatku VAT.

Kontrola i audyt mogą zapobiec udziałowi w nielegalnych procederach, mogą pomóc odkryć przestępcze działanie zorganizowanej grupy, ale – jak nie po raz pierwszy na Kongresie przypominano – ani audytor ani kontroler nie mogą zastępować organów ścigania dla dobra własnego, swojej organizacji i śledztwa.

Na Kongresie nie mogło zabraknąć najgorętszego tematu: zagrożeń, jakie na firmy czyhają w cyberprzestrzeni. Wśród najcenniejszych dóbr przedsiębiorstwa wskazuje się informację. Przechowywana w systemach informatycznych, funkcjonująca w świecie wirtualnym narażona jest na różnego rodzaju ataki. Polska administracja rządowa za podstawowy element ochrony zbieranych i przetwarzanych informacji uznaje dostosowanie systemu zarządzania bezpieczeństwem informacji do wymogów zawartych w normie PN-ISO/IEC27001:2007. Poszczególne państwa próbują wyznaczyć własny obszar cyberprzestrzeni i zbudować system jej ochrony i obrony, ale nie jest to proste, bo w świecie wirtualnym nie ma granic, nawet umownych. Monitorując cyberzagrożenia trzeba kontrolować zarówno zagrożenia wewnętrzne jak i zewnętrzne, bo nigdy nie wiadomo, skąd może nastąpić cyberatak. ✓

