www.pwc.com/crimesurvey

Badanie przestępczości gospodarczej Polska 2011

Cyberprzestępczość rosnącym zagrożeniem w biznesie

Listopad 2011

pwc

Wprowadzenie

Listopad 2011

Mamy przyjemność przedstawić Państwu polską edycję szóstego już badania przestępczości gospodarczej Global Economic Crime Survey 2011 (GECS 2011) prowadzonego przez PwC (wcześniej PricwaterhouseCoopers). Tegoroczny raport pokazuje jak zmieniła się przestępczość gospodarcza w Polsce w ostatnich dwóch latach i jakich trendów w zakresie nadużyć należy spodziewać się w dłuższej perspektywie. Ponadto, w raporcie podjęliśmy próbę oceny skuteczności mechanizmów kontrolnych i innych środków, którymi organizacje posługują się obecnie w celu identyfikacji nadużyć. Staraliśmy się wskazać kierunki zmian, które w naszej ocenie są niezbędne do poprawy efektywności mechanizmów obrony, a tym samym zbliżenia polskich organizacji do standardów światowych.

W tym roku raport podzielony jest na dwie główne części, dotyczące:

- obecnego środowiska nadużyć, w tym rodzajów popełnianych oszustw, sposobów ich wykrywania, ich skutków i sprawców;
- cyberprzestępczości – w której przedstawiamy m.in. ocenę świadomości organizacji w zakresie tego typu przestępstw i działania podejmowane przez przedsiębiorstwa w celu zwalczania i zapobiegania cyberprzestępczości.

W ciągu ostatnich 12 miesięcy 39% respondentów w Polsce doświadczyło przestępstwa gospodarczego. Aż 26% z poszkodowanych przyznała, że w ciągu ostatniego roku padła ofiarą cyberprzestępczości, która staje się coraz ważniejszym zjawiskiem na naszym rynku. Jednocześnie prawie połowa wszystkich respondentów w Polsce oceniła, iż wzrosła ich świadomość zagrożeń związanych z cyberprzestępczością.

Tegoroczne badanie pokazuje, iż efektywność narzędzi stosowanych przez Polskie organizacje do zapobiegania i wykrywania przestępstw jest niska. Wykrywanie nadużyć w coraz mniejszym stopniu jest rezultatem świadomego działania organizacji, stając się częściej dziełem przypadku – w ten sposób wykryło przestępstwa 16% organizacji w Polsce, czyli dwukrotnie więcej niż na świecie. Niewiele, bo zaledwie 3% nadużyć w Polsce zostało wykrytych za pomocą systemów zarządzania ryzykiem nadużyć (na świecie 10%), bądź też dzięki anonimowym informatorom, pochodzącym z wewnątrz, bądź z zewnątrz firmy, lub poprzez systemy whistleblowingu (łącznie wykryto tak 9% nadużyć w Polsce, 22% na świecie). W polskich organizacjach brakuje skutecznych narzędzi wykrywania i monitorowania przestępstw.

Brak odpowiednich narzędzi oznacza również brak możliwości oszacowania finansowych i pozafinansowych skutków nadużyć. Trend ten jest szczególnie niepokojący w dobie rosnącego zagrożenia cyberprzestępczością, w przypadku której - wraz z postępem technologii – wykrycie, pomiar skutków, czy też identyfikacja sprawcy staje się coraz trudniejsza.

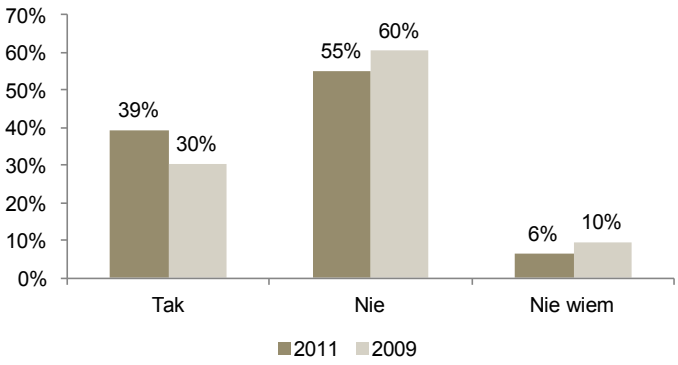
Wierzymy, że raport ten spełnił główny cel badania – udało nam się dokonać diagnozy zjawiska przestępczości gospodarczej w obecnej sytuacji ekonomicznej oraz wskazać kierunki zmian niezbędnych w organizacjach do skuteczniejszej walki z nadużyciami. Bardzo dziękujemy wszystkim organizacjom, które uczestniczyły w badaniu, bez których ten raport nie mógłby powstać. Co najważniejsze, mamy nadzieję, że nasze obserwacje pozwolą organizacjom skuteczniej walczyć z zagrożeniami związanymi z przestępczością gospodarczą.

Dariusz Cypcer

Dyrektor, Usługi Forensic, PwC

Wzrost odsetka organizacji, które stały się ofiarą przestępstw gospodarczych

Rys. 1: Wystąpienie przypadków nadużyć wśród polskich organizacji



Dlaczego wzrosła liczba organizacji dotkniętych nadużyciami?

W 2011 r., 39% badanych organizacji w Polsce przyznało, że doświadczyło zjawiska przestępstwa gospodarczego w ciągu ostatnich 12 miesięcy, co oznacza wzrost o 9 punktów procentowych (p.p.) w porównaniu z rokiem 2009 [por. Rys.1.].

Należy przy tym pamiętać, że przedstawiony w naszym raporcie poziom występowania oszustw gospodarczych zależy w praktyce od kombinacji dwóch czynników:

- obiektywnych zmian w poziomie przestępczości gospodarczej oraz
- skuteczności wykrywania oszustw przez przedsiębiorców.

Z naszego doświadczenia wynika, że kryzys ekonomiczny i spowolnienie gospodarcze mają bezpośredni wpływ na wzrost poziomu przestępczości gospodarczej. Obserwujemy wtedy z jednej strony rosnącą presję po stronie sprawców (spadające dochody, rosnące wydatki osobiste, itp.) a z drugiej strony postępujące ograniczanie mechanizmów kontrolnych (np. podziału obowiązków) wynikające z redukcji etatów u przedsiębiorców.

Oszczędności wprowadzane przez przedsiębiorców w czasach spowolnienia gospodarczego w pierwszej kolejności dotyczą funkcji administracyjnych, w tym komórek zajmujących się zapobieganiem i wykrywaniem nadużyć, co zmniejsza efektywność wykrywania oszustw. Niską efektywność narzędzi wykrywających nadużycia potwierdzają zresztą sami respondenci. Przedłużający się okres spowolnienia i obawy co do wystąpienia drugiej fali kryzysu dodatkowo nasilają powyższe tendencje.

Malejąca skuteczność wykrywania nadużyć nakazuje przypuszczać, że rzeczywisty wzrost przestępczości gospodarczej może być nawet większy niż widoczne w badaniu 9 p.p.

Dodatkowo, alarmującym sygnałem jest fakt, iż w Polsce nadużycia gospodarcze występują obecnie częściej niż w Europie Środkowo-Wschodniej oraz na świecie:

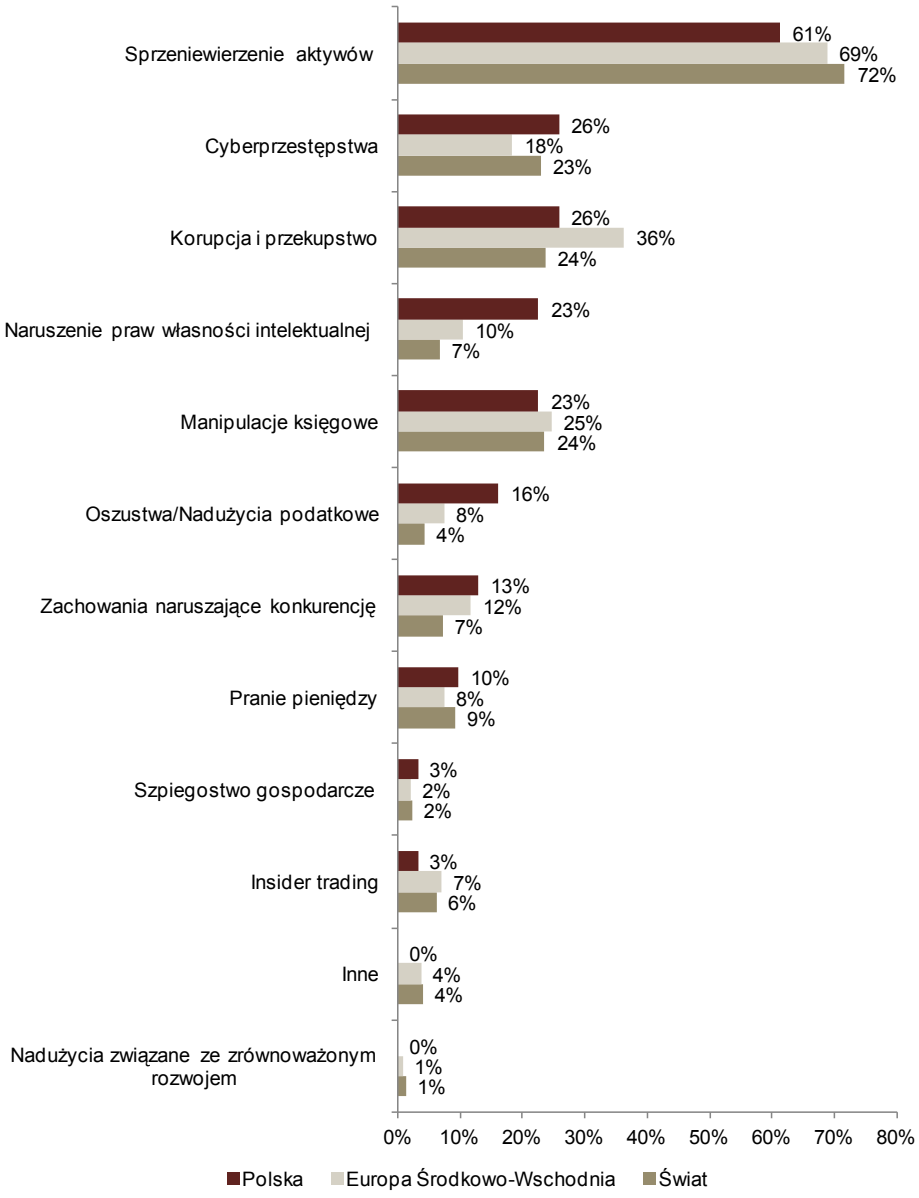
- w 2011 r. 0dsetek poszkodowanych organizacji w Europie Środkowo-Wschodniej wynosił 30%, a wśród organizacji na świecie 34%, czyli odpowiednio o 9 p.p. i 5 p.p. mniej niż w Polsce;
- wzrost przestępczości w Polsce w 2011 w porównaniu z rokiem 2009 (o 9 p.p.), był dwa razy większy niż na świecie gdzie wzrost wyniósł 4p.p. Dla odmiany w Europie Środkowo-Wschodniej odnotowano spadek zgłoszonej przestępczości (z 34% 2009 do 30% w 2011), kosztem wzrostu liczby firm, które nie potrafiły określić czy doświadczyły przestępstw (z 6% w 2009 do 9% w 2011).

Które rodzaje przestępstw w 2011 r. wystąpiły najczęściej?

Przestępstwa gospodarcze mogą przyjąć różne formy, niektóre są bardziej powszechne i bardziej trwałe niż inne. Rysunek 2 pokazuje rodzaje przestępstw gospodarczych, których ofiarą padły w ciągu ostatniego roku polskie organizacje.

Najczęściej występującym przestępstwem w Polsce było w 2011 r. sprzeniewierzenie aktywów – doświadczyło go 61% poszkodowanych organizacji. W porównaniu z rokiem 2009, odsetek ten był o 8 p.p. wyższy [por. Rys 3], wciąż jednak nieco niższy niż w organizacjach w Europie Środkowo-Wschodniej i na świecie (odpowiednio 69% i 72%).

Rys. 2: Rodzaje przestępstw gospodarczych



W dalszej kolejności polskie organizacje wskazały korupcję i przekupstwo (26% poszkodowanych organizacji) oraz cyberprzestępczość (również 26%).

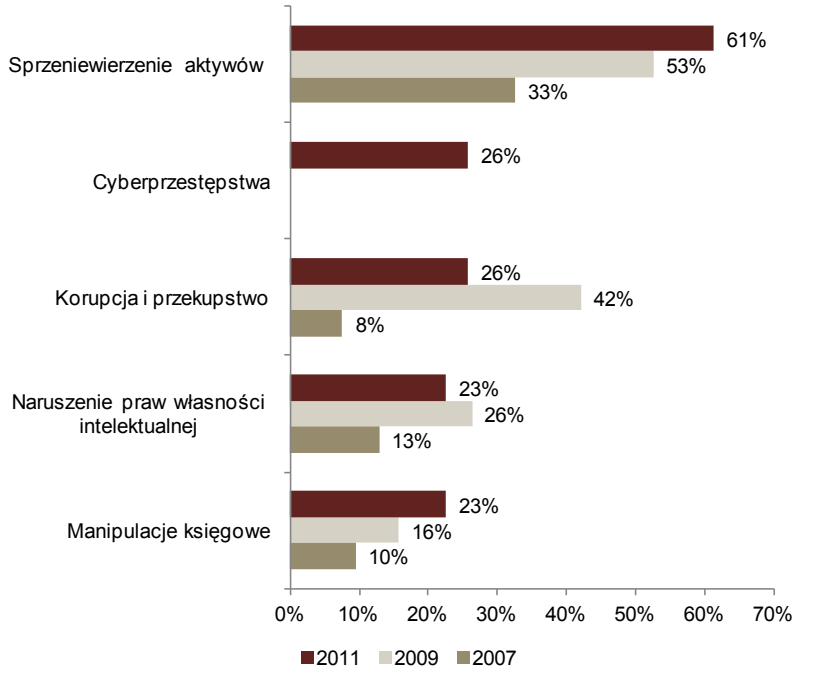
W 2011 r., w porównaniu z rokiem 2009, zdecydowanie mniej organizacji w Polsce doświadczyło korupcji i przekupstwa – spadek wynosi niemal 16 p.p. [por. Rys 3]. Zmiana ta może wynikać m.in. z nagłośnienia w mediach przypadków korupcji oraz spadku tolerancji społecznej na ten rodzaj przestępstw, co mogło skłonić organizacje do ostrożności i unikania sytuacji sprzyjających korupcji i łapówkarstwu, mogło również zniechęcić je do informowania o styczności z tym zjawiskiem. Warto zauważyć, iż na tle Europy Środkowo-Wschodniej Polska plasowała się zdecydowanie korzystniej – w krajach naszego regionu częstotliwość występowania korupcji i przekupstwa w 2011 r. była niemal o 10 p.p. większa niż w Polsce.

Stosunkowo nowym zjawiskiem na naszym rynku jest cyberprzestępczość, która w 2011 roku wystąpiła w aż 26% poszkodowanych organizacji, czyli częściej niż średnio w Europie Środkowo-Wschodniej i na świecie, gdzie odsetek wynosił odpowiednio 18% i 23% przedsiębiorstw. Wraz z rozwojem technologii organizacje coraz częściej stają się celem ataku cyberprzestępców, ponadto tak wysoki wynik był częściowo rezultatem zwiększonej uwagi mediów w odniesieniu do tej kategorii przestępstw – co mogło pomóc organizacjom odróżnić cyberprzestępczość od innych kategorii przestępstw i identyfikować jej przypadki. Szerzej przyglądamy się temu zjawisku w oddzielnej części raportu poświęconej cyberprzestępstwom.

Manipulacje księgowe wykryte przez 23% polskich organizacji okazały się w 2011 r. problemem o nieco większej skali niż jeszcze dwa lata wcześniej, kiedy to w Polsce wskazało je nieco ponad 16% badanych [por. Rys 3]. Niepewność sytuacji na rynkach finansowych i groźba utraty płynności przez organizacje powoduje presję na poprawę wyników finansowych, co sprzyja tego typu manipulacjom. Obecny poziom 23% jest porównywalny ze skalą zjawiska obserwowaną w Europie Środkowo -Wschodniej i na świecie.

Problemami charakterystycznymi dla polskiego rynku, w porównaniu z Europą Środkowo-Wschodnią i średnią globalną pozostaje naruszenie praw własności intelektualnej oraz oszustwa podatkowe. W Polsce nadużyć tego typu doświadczyło 2 razy więcej organizacji niż w Europie Środkowo-Wschodniej i 3 razy więcej niż na świecie.

Rys. 3: Pięć najczęściej występujących nadużyć w 2011 roku - trendy zmian



13% organizacji w Polsce w wyniku nadużyć poniosło straty powyżej 5mln USD

$5m

Mierzalne i niemierzalne koszty nadużyć

Jakie straty finansowe poniosły organizacje?

Pomimo że w 2011 r. więcej organizacji doświadczyło przypadków nadużyć niż w 2009 r., szacowane straty finansowe przez organizacje wydają się zmniejszać w ciągu tych dwóch lat zarówno w Polsce, jak i Europie Środkowo-Wschodniej oraz na świecie.

Wielkość strat w 2011 roku uległa „przesunięciu" w kierunku strat o niższych wartościach. W 2011 r. 42% organizacji dotkniętych nadużyciami w Polsce szacowało wartość wymiernych strat na kwotę mniejszą niż 100.000 USD, podczas gdy w 2009 r. ten odsetek wynosił 31%. Natomiast 13% polskich przedsiębiorstw w 2011 r. mówiło o stratach powyżej 5 mln USD- dla porównania w 2009 r. mówiło tak 16% organizacji. Co ciekawe, w 2011 r. na świecie odsetek organizacji dotkniętych nadużyciami, które poniosły straty powyżej 5 mln USD był mniejszy niż w Polsce i wynosił 10%.

Jakie były niemierzalne skutki nadużyć?

Oprócz mierzalnych strat ponoszonych przez przedsiębiorców na skutek nadużyć, ponoszą oni również koszty, których wartość trudno oszacować. Jako najistotniejsze polscy przedsiębiorcy wskazali: wpływ na morale pracowników (36% przedsiębiorców uznało ten czynnik jako istotny) i wpływ na reputację lub markę (19%) [por. Rys. 4.].

Istotny wzrost wskazań w odniesieniu do morale pracowników zbliżył wyniki polskiego badania do wyników ogólnoświatowych (odpowiedziała tak 1/3 organizacji na świecie).

Rys. 4: Niemierzalne koszty nadużyć

Istotny wzrost liczby nadużyć wewnątrz organizacji

69% nadużyć wewnątrz organizacji zostało popełnionych przez kadrę kierowniczą

Kim byli sprawcy nadużyć?

Jednym z podstawowych wyzwań w walce z przestępczością gospodarczą jest zgromadzenie informacji o sprawcach nadużyć. Wiedza na temat tego, kim są sprawcy i jak dokonują przestępstw pomaga w określeniu słabych punktów w mechanizmach reagowania i kontroli wewnętrznej stosowanych w przedsiębiorstwach. Ponieważ skala nadużyć wzrasta, organizacje muszą być coraz bardziej aktywne w działaniach mających na celu obronę przed atakami. Na podstawie informacji od przedsiębiorstw, które doświadczyły przestępczości gospodarczej sporządziliśmy profil typowego sprawcy najbardziej poważnych przestępstw.

W Polsce w porównaniu z rokiem 2009, w 2011 r. istotnie wzrósł udział nadużyć dokonanych przez osoby z wewnątrz organizacji, czyli jej pracowników. W 2009 r. tego typu nadużycia dokonane przez sprawców wewnętrznych stanowiły jedynie 26% wszystkich wykrytych przestępstw gospodarczych, podczas gdy w 2011 r. stanowiły one 42% wykrytych przestępstw.

W 2011 r. sprawcy wewnętrzni rekrutowali się przede wszystkim z kadry kierowniczej średniego i wyższego szczebla (69% nadużyć wewnętrznych). Analizując grupę sprawców pochodzących z zewnątrz organizacji, najczęściej do nadużycia dochodziło ze strony klientów (tak wskazało 47% organizacji, które padły ofiarą nadużyć z zewnątrz), agentów lub pośredników (18%) oraz dostawców (12%).

Zaostrzenie środków podejmowanych wobec sprawców nadużyć wewnętrznych; środki wobec sprawców zewnętrznych są łagodniejsze

Tab.1: Działania podjęte przez organizacje w stosunku do sprawców nadużyć

	Sprawcy nadużyć wewnętrznych		Sprawcy nadużyć zewnętrznych	
Środki podjęte wobec sprawców	2011	2009	2011	2009
Zwolnienie pracownika / zakończenie współpracy z partnerem	77%	48%	53%	68%
Sądowe postępowanie cywilne wraz z egzekucją	54%	42%	53%	58%
Zawiadomienie organów ścigania	54%	n/a	53%	n/a
Zawiadomienie odpowiednich służb nadzorujących	31%	26%	65%	42%
Ostrzeżenie / nagana	23%	26%	n/a	n/a
Przeniesienie pracownika	0%	5%	n/a	n/a
Nie podjęła żadnych działań	0%	0%	6%	0%
Inne	0%	5%	6%	5%

Jakie środki podjęto wobec sprawców?

W związku z rosnącą skalą przestępstw wewnętrznych przedsiębiorstwa zaostrzyły konsekwencje podejmowane wobec sprawców tych nadużyć w porównaniu do 2009 r.:

- w 2011 r. aż 77% organizacji podjęło decyzję o zwolnieniu wewnętrznego sprawcy nadużyć, podczas gdy w 2009 r. na ten krok zdecydowało się jedynie 48% badanych organizacji [por. Tab.1.];
- ponadto ponad połowa organizacji, które doświadczyły nadużyć ze strony pracowników zdecydowało się na podjecie kroków prawnych – wszczęcie sądowego postępowania cywilnego wraz z egzekucją lub zawiadomienie organów ścigania (54% badanych organizacji) [por. Tab.1.].

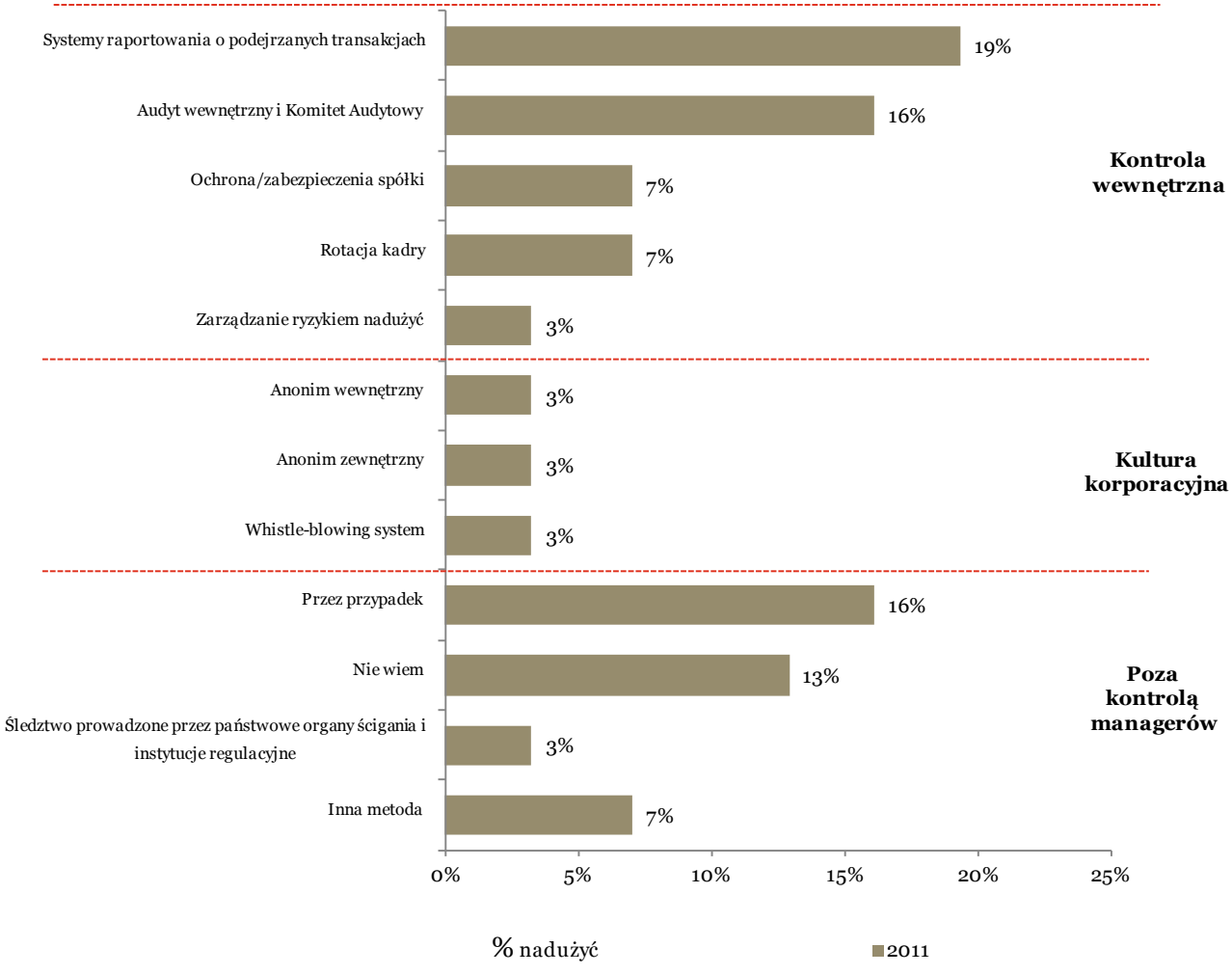
Co ciekawe, w odniesieniu do sprawców zewnętrznych środki podejmowane w 2011 r. przez poszkodowane organizacje wydają się mniej dotkliwe niż stosowane w 2009 r. W 2011 r. aż 6% organizacji, które ucierpiały w wyniku nadużycia ze strony podmiotu zewnętrznego nie wyciągnęło żadnych konsekwencji wobec sprawcy. Dla porównania, w 2009 r. żadna z poszkodowanych organizacji nie zaniechała działań wobec sprawców zewnętrznych.

Ponadto w 2011 r. przedsiębiorstwa rzadziej niż w roku 2009 decydowały się na zakończenie współpracy z nieuczciwym partnerem – w 2009 r. krok ten podjęło 68% organizacji dotkniętych nadużyciem, a w 2011 r. już tylko 53%. W 2011 r., nieco mniejszy niż dwa lata wcześniej odsetek organizacji zdecydował się na podjęcie kroków prawnych – postępowanie sądowe wraz z egzekucją.

Z drugiej strony w 2011 r., w porównaniu do 2009 r. organizacje częściej decydowały się na zawiadomienie odpowiednich służb nadzorujących (wzrost z 42% do 65%). Mamy tu na myśli informowanie o przypadkach nadużyć zarówno Rad Nadzorczych, jak również zewnętrznych organów regulacyjnych, takich jak KNF.

Brak sprawnie funkcjonujących mechanizmów wykrywania przestępstw

Rys.5: Metody wykrywania nadużyć



Coraz więcej nadużyć wykrywanych jest za pomocą mechanizmów będących poza kontrolą spółki

Wykrywanie nadużyć

Oszustwa mogą zostać wykryte za pomocą mechanizmów i procedur istniejących w organizacji, lub też niezależnie od nich. Główne sposoby ujawniania nadużyć obejmują:

- kontrole wewnętrzne spółki, takie jak audyt wewnętrzny, zarządzanie ryzykiem nadużyć, elektroniczne lub automatyczne systemy zgłaszania podejrzanych transakcji, ochronę i zabezpieczenia spółki lub na skutek rotacji pracowników (zmiany personelu / obowiązków);
- elementy odnoszące się do kultury korporacyjnej, obejmujące m.in. jawne lub poufne informowanie o zdarzeniach pochodzące z wewnątrz lub z zewnątrz organizacji, bądź specjalne systemy whistleblowingu służące do anonimowego informowania o nadużyciach przez pracowników;
- elementy będące poza kontrolą spółki, takie jak np. przypadek, śledztwa podejmowane przez organy ścigania.

Rysunek nr 5 przedstawia jak polskie organizacje wykrywały oszustwa w 2011 r.

Jak wyglądały metody detekcji w Polsce?

Największa część nadużyć w Polsce została wykryta dzięki rutynowym mechanizmom kontroli wewnętrznej takim jak: monitorowanie podejrzanych transakcji (19% organizacji), bądź też przez audyt wewnętrzny / Komitet Audytowy (16% organizacji).
Te dwie formy wykrywania nadużyć dominowały również na świecie.

Elektroniczne lub automatyczne monitorowanie i raportowanie podejrzanych transakcji jest zwykle stosowane do wykrywania, śledzenia i zwalczania oszustw w sektorze usług finansowych, gdzie wykorzystuje się wysoko zaawansowane narzędzia, oparte na elektronicznych zautomatyzowanych systemach działających bez ingerencji człowieka. W 2011 r. udział przestępstw wykrytych przy pomocy takich systemów raportowania istotnie wzrósł w stosunku do wcześniejszych lat (z 4% w 2007 r. do 19% w 2011 r.). Jednocześnie znacznie spadł udział oszustw wykrytych przez audyt wewnętrzny (z 26% w 2007 r., 22% w 2009 r. do 16% w 2011 r.). Zmiany te można wyjaśnić z jednej strony postępem technologicznym w zakresie budowy systemów detekcji, z drugiej natomiast redukcją etatów w pionach administracyjnych przedsiębiorstw (w tym w departamentach audytu wewnętrznego), będącą reakcją na pogarszającą się sytuację ekonomiczną.

Co świadczy o niskiej efektywności mechanizmów detekcji?

Coraz większa część nadużyć jest w Polsce wykrywana za pomocą mechanizmów znajdujących się poza kontrolą spółki. W 2011 r. przez przypadek odkrytych zostało w Polsce aż 16% nadużyć, czyli dwukrotnie więcej niż ma to miejsce w organizacjach na świecie, natomiast aż 13% organizacji nie potrafiło wskazać, w jaki sposób zidentyfikowało nadużycie. Wydaje się to konsekwencją redukcji kosztów oraz braku sprawnie funkcjonujących mechanizmów i systemów służących wykrywaniu oraz raportowaniu przestępstw, takich jak system zarządzania ryzykiem nadużyć lub systemy whistleblowingu.

Ze wszystkich organizacji w Polsce, które doświadczyły nadużyć, jedynie 3% odkryło je poprzez systemy zarządzania ryzykiem nadużyć (Fraud Risk Management), natomiast kolejne 3% za pomocą formalnych systemów poufnego informowania (systemy whistleblowingu). Na świecie obie metody przyczyniły się do wykrycia łącznie 15% przestępstw.

Aż 38% polskich organizacji nie posiada systemów whistleblowingu, natomiast 45% organizacji, w których takie systemy funkcjonują, ocenia je jako nieefektywne lub mało efektywne. Dodatkowo, w porównaniu z rokiem 2009, obserwujemy istotny spadek wykrywania nadużyć poprzez nieformalne anonimowe informowanie – w 2009 dzięki anonimom wewnętrznym i zewnętrznym łącznie nadużycia wykryło 27% poszkodowanych organizacji, obecnie tylko 6%. Brak popularności tych metod wykrywania przestępstw w Polsce świadczy o braku miejsca w obecnej kulturze korporacyjnej organizacji na metody anonimowego informowania o przestępstwach. Wielu ta metoda informowania kojarzy się pejoratywnie – z donosicielstwem. Ponadto organizacje często nie są w stanie zagwarantować anonimowości informatorom.

Jednym z narzędzi wspierających mechanizmy wykrywania przestępstw przez organizacje jest dokonywanie ocen ryzyka nadużyć (fraud risk assessment) – w 2011 r. 71% nadużyć zostało wykrytych w Polsce właśnie przez organizacje dokonujące takich ocen. Niemniej jednak, aż 37% wszystkich badanych organizacji w Polsce w ciągu ostatnich 12 miesięcy nie zdecydowała się na przeprowadzenie oceny ryzyka nadużyć bądź nie potrafiła powiedzieć czy taką ocenę przeprowadzono. Najczęstszą przyczyną zaniechania ocen był brak wiary w jej wartość i brak wiedzy, czym ona jest.

Ogólna percepcja występowania nadużyć istotnie wzrosła

Zmiany w percepcji nadużyć

Ogólna percepcja zagrożeń związanych z nadużyciami gospodarczymi w 2011 r. wzrosła w porównaniu z rokiem 2009 – dla większości rodzajów nadużyć organizacje częściej niż w 2009 r. oceniały, że możliwość ich wystąpienia jest prawdopodobna [por. Tab.2.], przewidują zatem iż skala przestępstw w przyszłości jeszcze wzrośnie.

Tab.2: Percepcja a rzeczywiste przypadki nadużyć w 2011

Rodzaj nadużyć	Przypadki nadużyć	Percepcja nadużyć
Sprzeniewierzenie aktywów	61%	30%
Cyberprzestępstwa	26%	34%
Korupcja i przekupstwo	26%	28%
Naruszenie praw własności intelektualnej	23%	37%
Manipulacje księgowe	23%	14%
Oszustwa / nadużycia podatkowe	16%	14%
Zachowania naruszające konkurencję	13%	24%
Pranie pieniędzy	10%	15%
Szpiegostwo gospodarcze	3%	22%
Insider trading	3%	6%
Nadużycia związane ze zrównoważonym rozwojem	0%	5%
Inne	0%	4%

Biorąc pod uwagę, że postrzeganie przestępczości gospodarczej nie odpowiada rzeczywistej skali tego zjawiska, zadaliśmy organizacjom pytanie na ile prawdopodobne jest, że ich organizacja doświadczy wybranych przestępstw gospodarczych w ciągu następnych 12 miesięcy. Jako prawdopodobne najwięcej polskich organizacji wskazało wystąpienie: naruszenia praw własności intelektualnej (37%), cyberprzestępstw (34%), sprzeniewierzenia aktywów (30%), na czwartym zaś miejscu korupcji i przekupstwa (28%). Są to jednocześnie 4 najczęściej występujące przestępstwa w Polsce 2011 r. [por. Tab.2.].

Rozbieżności pomiędzy percepcją a występowaniem nadużyć

Badania PwC wskazują, że istnieją wyraźne rozbieżności pomiędzy skalą rzeczywistego występowania pewnych kategorii nadużyć, a postrzeganiem tego typu zagrożeń przez polskich przedsiębiorców.

W przypadku sprzeniewierzenia aktywów – rzeczywiste występowanie jest wyraźnie wyższe niż percepcja, co może świadczyć o niedocenianiu przez przedsiębiorców "tradycyjnej" kradzieży, która w rzeczywistości jest najczęściej występującą kategorią nadużyć.

Z kolei szpiegostwo gospodarcze, cyberprzestępstwa, czy naruszanie zasad uczciwej konkurencji oraz własności intelektualnej są tymi przestępstwami, gdzie percepcja jest wyraźnie wyższa od ich rzeczywistego występowania. Takie sytuacje można interpretować bądź jako obawy „na wyrost" kreowane przez środki masowego przekazu, bądź jako rzeczywiste zagrożenia, które jednak nie są wykrywane ze względu na zbyt małe doświadczenie polskich przedsiębiorców przy tego typu nadużyciach.

Zmiana percepcji wraz z upływem czasu

Badania PwC pokazują, że w miarę upływu czasu różnice pomiędzy rzeczywistym występowaniem poszczególnych nadużyć a ich postrzeganiem wyrównują się. Z jednej strony przedsiębiorcy uczą się identyfikować poszczególne rodzaje przestępstw, a z drugiej strony percepcja staje się bardziej realna i oparta na racjonalnych przesłankach i własnych doświadczeniach.

Na przestrzeni ostatnich lat stało się tak w przypadku korupcji, której percepcja osiągnęła szczyt w badaniu z 2007 r. przy jednocześnie niskich wskaźnikach występowania. Jednak już w obecnym badaniu częstotliwość występowania tego przestępstwa prawie zrównała się z percepcją. W miarę upływu czasu zmniejsza się też różnica wskazań pomiędzy występowaniem i percepcją w odniesieniu do sprzeniewierzenia aktywów.

Wyraźnie widoczną tendencją w obecnej rzeczywistości biznesowej jest rosnąca rola oszustw związanych z postępem technologicznym – przede wszystkim cyberprzestępczości oraz w mniejszym stopniu – szpiegostwa gospodarczego. Ze względu na wagę problemu cyberprzestępczości zdecydowaliśmy się poświęcić temu zagadnieniu osobny rozdział naszego raportu.

Cyberprzestępczość

Pojęcie cyberprzestępczości nie zostało do tej pory jednoznacznie zdefiniowane i podlega różnym interpretacjom. Dla celów naszego badania przyjęliśmy następującą definicję cyberprzestępczości:

„Cyberprzestępczość, znana również, jako przestępczość komputerowa, to przestępstwo gospodarcze popełnione przy użyciu komputera i Internetu. Typowymi przypadkami cyberprzestępczości są: rozpowszechnianie wirusów, nielegalne pobieranie plików, phishing i pharming oraz kradzież danych osobowych np. danych dotyczących kont bankowych i kart kredytowych. Wyklucza to rutynowe oszustwa, w których komputer został wykorzystany jako jedno z szeregu pobocznych narzędzi w celu ich popełnienia, obejmuje natomiast tylko takie przestępstwa gospodarcze, w których komputer, Internet lub wykorzystanie urządzeń i mediów elektronicznych jest podstawowym narzędziem."

Wzrost percepcji organizacji w Polsce odnośnie zagrożenia cyberprzestępczością

W 2011 r. cyberprzestępczość była jednym z trzech najczęściej występujących przestępstw w Polsce

Cyberprzestępczość w Polsce w 2011 r.

Zgodnie z wynikami badań PwC, cyberprzestępstwa – obok sprzeniewierzenia aktywów oraz korupcji i przekupstwa – znalazły się w 2011 r. w grupie trzech najczęściej występujących przestępstw gospodarczych.

W poprzednich edycjach badania, poziom odpowiedzi dotyczący cyberprzestępczości był tak niski, że nie występowała ona jako osobna kategoria nadużyć. W 2011 roku 1/4 organizacji doświadczyła w ciągu ostatniego roku przypadków cyberprzestępczości. Nasuwa się pytanie, w jaki sposób i dlaczego cyberprzestępczość stała się jednym z popularniejszych rodzajów oszustw. Niektórymi z możliwych przyczyn mogą być:

- większa uwaga mediów kierowana w stronę przypadków cyberprzestępczości, co doprowadziło do zwiększenia świadomości na temat tego rodzaju oszustw i mogło być przyczyną dodatkowych kontroli wdrożonych przez organizacje w tym obszarze, co z kolei mogło przyczynić się do wykrycia większej liczby przypadków tego rodzaju przestępstw;
- niejasności wokół definicji cyberprzestępczości co skutkowało tym, że respondenci mogli niewłaściwie klasyfikować niektóre z bardziej tradycyjnych typów przestępstw gospodarczych jako cyberprzestepczość, ponieważ zostały popełnione przy użyciu komputera, urządzeń elektronicznych lub Internetu;
- większy nacisk organów regulacyjnych na identyfikację i zapobieganie cyberprzestępstwom;
- postęp w technologii, ułatwiający popełnianie cyberprzestępstw.

37% organizacji ocenia, iż ryzyko związane z cyberprzestępczością wzrosło

37%

Ryzyka i zagrożenia związane z cyberprzestępczością

Bez względu na możliwe przyczyny dużej liczby zgłoszonych przypadków, 37% polskich organizacji ocenia, iż w ciągu ostatnich 12 miesięcy ryzyko związane z cyberprzestępczością wzrosło, podczas gdy tylko 10% organizacji zauważa tendencję odwrotną. Percepcja w zakresie zagrożenia cyberprzestępczością zmieniła się także w ciągu ostatnich dwóch lat na świecie i w Europie Środkowo-Wschodniej – odpowiednio 40% i 30% organizacji jest przekonanych o większym zagrożeniu przestępczością komputerową.

Co więcej, 34% polskich organizacji ocenia, iż jest prawdopodobne, że padnie ofiarą cyberprzestępstwa w ciągu następnych 12 miesięcy. W tym przypadku, percepcja zagrożenia jest wyższa niż rzeczywiste przypadki nadużyć odnotowane w 2011 r. (26%).

Dlaczego zagrożenie cyberprzestępczością wzrasta?

Jednym z powodów rosnącego poczucia zagrożenia ze strony cyberprzestępczości jest większa trudność w ujęciu sprawców w porównaniu z przestępczością tradycyjną, wynikająca z tego, że:

- cyberprzestępstwo może być popełnione z dowolnego miejsca i w dowolnym czasie – co oznacza, że sprawca nie musi być fizycznie obecny w miejscu przestępstwa, co zmniejsza szansę złapania go na gorącym uczynku;
- istnieje mniejsze prawdopodobieństwo identyfikacji sprawcy przez organy ścigania bądź określenia, gdzie sprawca przebywał w momencie popełnienia przestępstwa; sprawca może znajdować się poza granicami kraju, w którym organizacja ma siedzibę, a tym samym jego identyfikacja i podjęcie tradycyjnych czynności śledczych zmierzających do jego ścigania i zatrzymania mogą okazać się bardzo trudne, czasem nawet niemożliwe;
- w wyniku szybkiego rozwoju technologii, cyberprzestępczość wciąż ewoluuje – co sprawia, że obowiązujące przepisy prawne nie są wystarczająco dojrzałe, a ich siła oddziaływania jest często niewystarczająca, aby ścigać cyberprzestępców. Dlatego w zakresie prawodawstwa i polityki korporacyjnej ryzyka związane z cyberprzestępczością powinny podlegać stałej ocenie i monitorowaniu, zaś metody jej zapobiegania – powinny być dostosowywane do tempa jej rozwoju.

Czego obawiają się polskie organizacje?

Największy niepokój polskich organizacji w odniesieniu do cyberprzestępczości wywołują ryzyka:

- kradzieży własności intelektualnej, w tym kradzieży danych (1/3 polskich organizacji);
- kradzieży lub utraty danych osobowych (1/3 organizacji);
- przerwy w świadczeniu usług (1/3 organizacji);
- utraty reputacji (1/3 organizacji);
- strat finansowych (1/5 organizacji).

Z kolei zarówno w Europie Środkowo-Wschodniej jak i na świecie najwięcej organizacji najbardziej obawia się utraty reputacji (odpowiednio 34% i 40% organizacji), nieco mniej kradzieży i utraty danych.

tylko 23% organizacji deklaruje regularny monitoring ryzyk związanych z cyberprzestępczością

23%

Środki zaradcze, w tym monitoring mediów

W jaki sposób organizacje zarządzają ryzykiem cyberprzesteptsw?

Bieżące zarządzanie cyber-bezpieczeństwem powszechnie ulokowane jest w ramach działów IT lub bezpieczeństwa.

W sytuacji wystąpienia przypadku cyberprzestępstwa większość polskich organizacji zamierza skorzystać z wewnętrznych zasobów organizacji – 75% organizacji deklaruje, że przeprowadzi wewnętrzne konsultacje z doświadczonymi pracownikami w celu wyjaśnienia sprawy.

Duży odsetek polskich organizacji skorzysta z pomocy zewnętrznej – 62% organizacji zawiadomi organy ścigania, a 60% przeprowadzi zewnętrzne konsultacje z ekspertami. W porównaniu do polskich, organizacje z Europy Środkowo-Wschodniej i organizacje na świecie rzadziej zadeklarowały powiadomienie organów ścigania, nieco częściej zaś – wewnętrzne konsultacje z pracownikami.

W Polsce jedynie 23% organizacji deklaruje regularny monitoring ryzyk związanych z cyberprzestępczością. Nie jest również popularne rozszerzanie świadomości pracowników w odniesieniu do cyberprzestępczości:

- 42% badanych organizacji w ciągu ostatnich 12 miesięcy w żaden sposób nie informowało pracowników o ryzyku cyberprzestępczości;
- 33% organizacji w Polsce informowała pracowników w formie ogłoszeń, natomiast 30% organizacji – w formie prezentacji lub warsztatów;
- 15% organizacji przeprowadziło szkolenia komputerowe w tym zakresie.

Organizacje nie były w stanie jednoznacznie ocenić skuteczności komunikowania ryzyk związanych z cyberprzestępczością, niemniej jednak szkolenia komputerowe uznane zostały za najbardziej efektywny sposób informowania pracowników.

Co można zrobić, aby skuteczniej zredukować to ryzyko?

Przedsiębiorcy nie do końca wiedzą, w jaki sposób minimalizować ryzyko cyberprzestępstw, podczas gdy podstawowe proste środki zaradcze mogą istotnie zredukować to ryzyko:

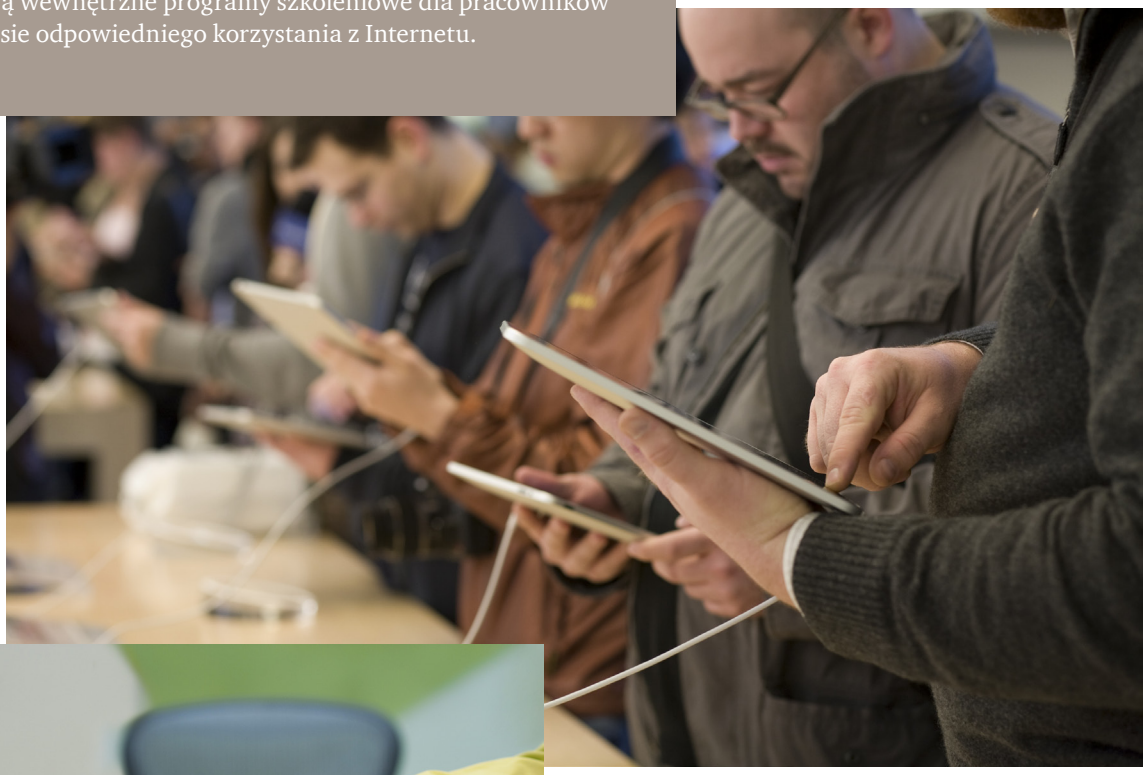
- zaangażowanie zarządu wyższego szczebla – w celu zwiększenia świadomości odnośnie zagrożeń cyberprzestępczością;
- zwiększenie świadomości organizacji oraz działania edukacyjne wobec pracowników;
- ocena funkcji bezpieczeństwa i przygotowania organizacji na przypadki cyberprzestępczości – w świetle dynamicznych zmian w technologii i zmieniających się zagrożeń ze strony cyberprzestępczości;
- dedykowanie zespołu, który będzie gotowy na działania w sytuacji zaistnienia przypadków cyberprzestępstw;
- przyjęcie przez organizacje zdecydowanej postawy wobec wykrytych cyberprzestępstw – zgłaszanie tego rodzaju przestępstw do organów regulacyjnych lub organów ścigania, wyciąganie konsekwencji prawnych itd.

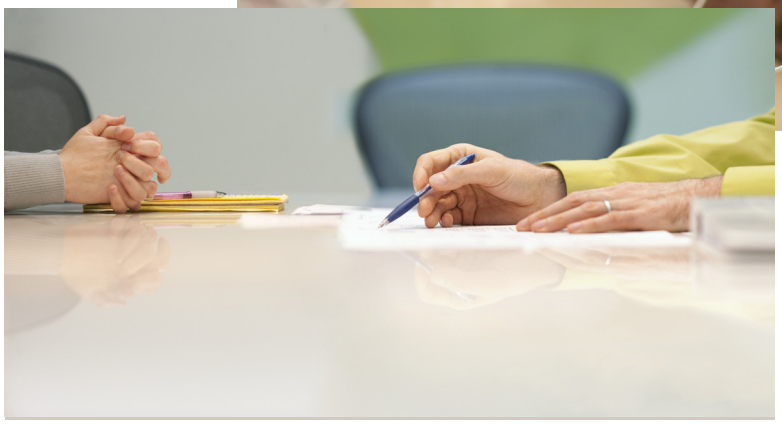
Monitorowanie serwisów społecznościowych przez organizacje

Choć portale społecznościowe takie jak Facebook, Twitter lub LinkedIn nie są bezpośrednim źródłem cyberprzestępczości, mogą one zwiększać jej zasięg lub efektywność. Na przykład, strony portali społecznościowych mogą zostać wykorzystane do zbierania informacji o konkretnych osobach (metoda określana jako „spear phishing"), do wyszukiwania informacji o pracownikach lub w celu zainstalowania złośliwego oprogramowania na komputerze użytkownika.

30% organizacji w Polsce (40% na świecie) prowadzi monitoring używania przez pracowników portali społecznościowych takich jak Facebook czy Twitter, które mogą stanowić zagrożenie dla organizacji.

W celu zwalczania zagrożeń związanych z używaniem portali społecznościowych oraz korzystaniem z sieci, organizacje monitorują wewnętrzny lub zewnętrzny ruch elektroniczny, w tym aktywności w Internecie (74% organizacji), umieszczają w umowach z pracownikami obowiązek właściwego korzystania z wewnętrznej dokumentacji i informacji (61% organizacji) oraz wdrażają wewnętrzne programy szkoleniowe dla pracowników w zakresie odpowiedniego korzystania z Internetu.





Podsumowanie

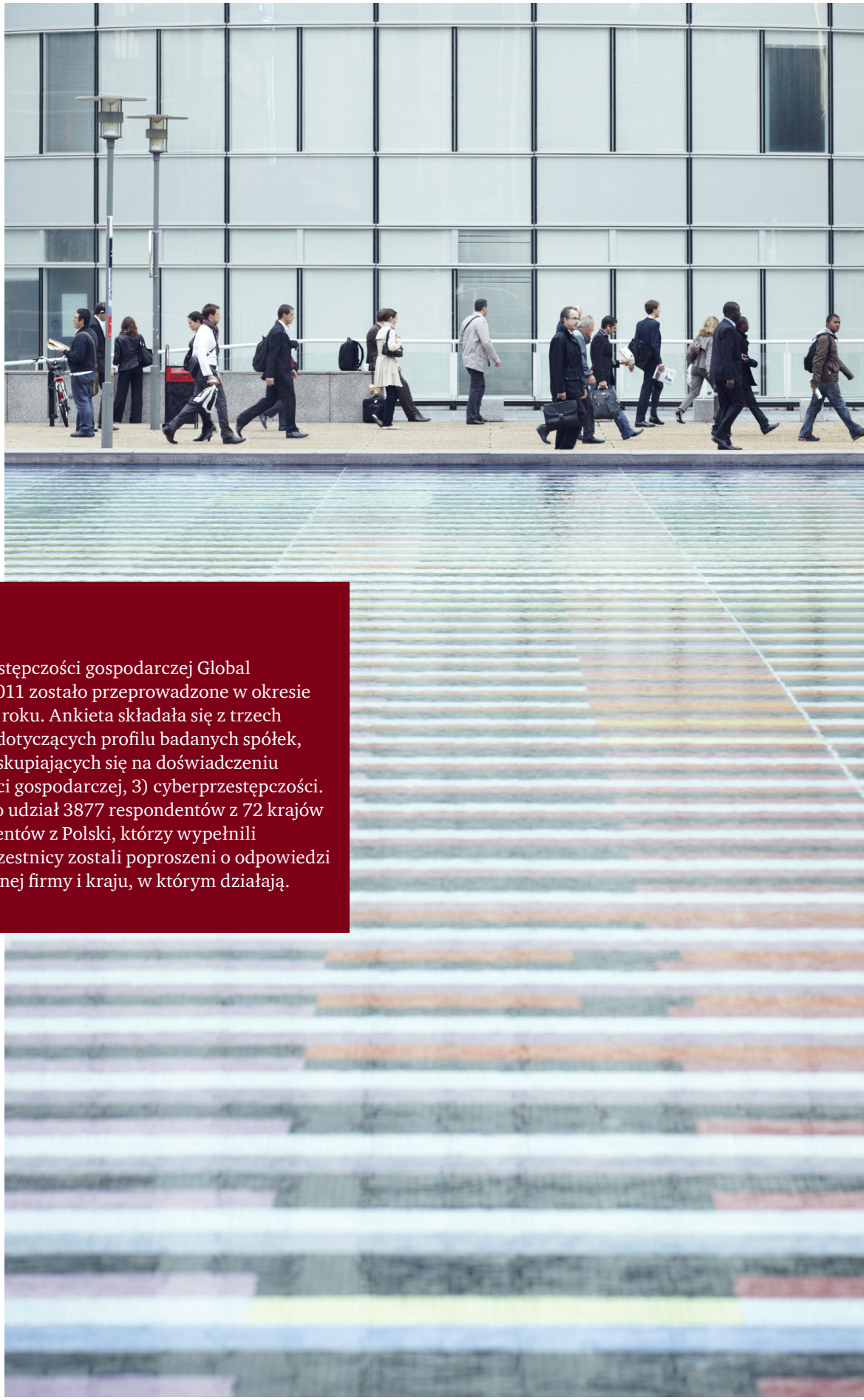
Organizacje powinny pozostawać czujne i podejmować aktywne działania na rzecz walki z nadużyciami

Wyniki tegorocznego badania pokazują, że nadużycia gospodarcze są trwałym zagrożeniem, z którym przegrywa coraz większy odsetek polskich organizacji. Dlatego powinny one pozostawać czujne i podejmować aktywne działania na rzecz walki z nadużyciami.

„Tradycyjne" oszustwa, jak sprzeniewierzenie aktywów, korupcja i przekupstwo, naruszanie własności intelektualnej czy manipulacje księgowe, pozostają w czołówce najczęściej występujących przestępstw. Ale rosną w siłę „nowe" rodzaje oszustw – w szczególności cyberprzestępstwa. Razem z nowoczesnymi formami prowadzenia biznesu, rozwojem nowych technologii i zmieniającym się środowiskiem pracy, pojawiają się nowe zagrożenia i sposoby dokonywania oszustw. Organizacje muszą mieć świadomość tych zmian i adekwatnie dostosowywać mechanizmy reakcji i metody wykrywania nadużyć. Dotyczy to w szczególności polskich organizacji, w których te mechanizmy wydają się nie funkcjonować efektywnie. Zwłaszcza w dobie redukcji zatrudnienia, która dotyka również stanowisk kontrolnych, istnieje ryzyko, że coraz więcej oszustw może pozostać nie wykrytych.

Niebezpieczeństwo to nabiera nowego znaczenia, w czasach coraz większej ingerencji nowoczesnych technologii w środowisko biznesowe. Smartfony, tablety, media społecznościowe – wszystkie oferują organizacjom wiele atrakcyjnych rozwiązań, ale mogą być również puszką Pandory, kryjącą niebezpieczeństwa. Urządzenia elektroniczne zawierają często poufne dane i informacje, które łatwo jest przenosić i równie łatwo stracić, jeśli nie są odpowiednio zabezpieczone. Ponadto miejsca dokonywania działań biznesowych i transakcji coraz częściej przenoszą się ze świata rzeczywistego do świata wirtualnego, który niesie ze sobą nowe ryzyka.

Zaawansowanie technologii postępuje szybko, podobnie jak umiejętności sprawców nadużyć, zostawiając wiele organizacji daleko w tyle. Dlatego bardzo ważnym jest, aby problemy informatyczne i związane z cyber-bezpieczeństwem miały zagwarantowane stałe miejsce w rejestrze ryzyk organizacji. Organizacje, które gotowe są zrozumieć i określić ryzyka i szanse, które niesie ze sobą świat wirtualny, będą pierwszymi, które uzyskają przewagę konkurencyjną w dzisiejszym napędzanym technologią świecie. Przykład idący „z góry", ze strony kierownictwa organizacji, jest kluczowym elementem w walce z przestępczością gospodarczą.



Metodologia

Nasze szóste badania przestępczości gospodarczej Global Economic Crime Survey 2011 zostało przeprowadzone w okresie od lipca do listopada 2011 roku. Ankieta składała się z trzech części: 1) pytań ogólnych dotyczących profilu badanych spółek, 2) pytań porównawczych skupiających się na doświadczeniu przypadków przestępczości gospodarczej, 3) cyberprzestępczości. W sumie w badaniu wzięło udział 3877 respondentów z 72 krajów świata, w tym 79 respondentów z Polski, którzy wypełnili kwestionariusz online. Uczestnicy zostali poproszeni o odpowiedzi na pytania dotyczące własnej firmy i kraju, w którym działają.

Kontakt

Dariusz Cypcer
Dyrektor, Usługi Forensic
tel. +48 22 523 4181
dariusz.cypcer@pl.pwc.com

Marcin Kossowski
Dyrektor, Forensic Services
tel. +48 22 523 4201
marcin.kossowski@pl.pwc.com

Marcin Klimczak
Starszy menedżer, Usługi Forensic
tel. +48 22 523 4087
marcin.klimczak@pl.pwc.com

Designed by Monika Mazur