

Стопанска престъпност: познати и нови заплахи за Вашия бизнес

Глобално проучване на
стопанската престъпност, 2014 г.

Резултатите за България

Глобално проучване
на стопанската
престъпност, 2014 г.
България

м.април 2014 г.



Съдържание

Въведение	3
Методология	3
Акценти	4
Измамата – представлява ли тя значителен риск за бизнеса в България?	5
Видове стопански престъпления – идентифицирани ли са нови рискове?	5
Най-разпространените измами	5
Нови видове измами	6
Възприемане и реалност – съществува ли разминаване?	8
Цената на измамата – трябва ли да се вземат предвид и „непреките (вторичните) щети“?	9
Разкриване на измами – ефективни ли са средствата за разкриване и предотвратяване на измами?	10
Типичният извършител – познавате ли врага си?	11
Противодействие спрямо извършителите – важна ли е бързата и адекватна реакция?	12
Терминология, използвана в доклада	13
Контакти за България	15

Въведение

Представяме на Вашето внимание резултатите от проведеното от ПрайсютърхаусКупърс Глобално проучване на стопанската престъпност 2014 г. – най-мощното проучване по рода си в световен мащаб. В нашето онлайн проучване взеха участие представители на висшето ръководство на 5,128 компании от цял свят, включително 79 водещи български организации, които ни предоставиха изключително ценна, по своята дълбочина и обхват, информация относно начина, по който стопанската престъпност се възприема от и влияе върху бизнеса по света и в България, в частност.

Методология

Седмото Глобално проучване на стопанската престъпност се проведе в периода от 4-ти септември 2013 г. до 25-ти октомври 2013 г. Въпросникът съдържаше общо 46 въпроса. От България взеха участие 79 организации от различни индустриални сектори като търговия на дребно, транспорт и логистика, производство, финансови услуги, енергетика, комунални услуги и добивна промишленост, строителство и инженерство и др.

63% от българските участници в проучването са частни компании, а 32% - публични дружества, търгувани на фондовата борса; останалите 5% не са посочили каква е структурата на собствеността в техните организации.

Данните в проучването са базирани изцяло на информацията, получена от участниците за случаите на стопански престъпления в техните организации, за различните видове стопански престъпления, на които те са били обект, за въздействието на тези престъпления върху организациите (както директните загуби, така и непреките („вторичните“) щети) за извършителите на престъпленията и за мерките, предприети от организациите след установяване на престъпленията.

С цел да се гарантира конфиденциалността на участниците, всички резултати от проучването са представени в обобщен вид, като са свързани само със съответната индустрия, големина на организацията и други статистически данни. Не са правени референции към конкретни организации.

Акценти

Измами

- 25% от анкетираните български организации са били обект на стопанско престъпление през последните две години.
- Всяка четвърта организация, жертва на измама, е претърпяла загуби на стойност над 100 хил. щатски долара (щ.д.).
- Присвояването на активи е най-разпространеният вид измама в България.
- Организацията възприемат корупцията като най-голяма заплаха за своя бизнес.
- Компютърните измами и измамите, свързани с поръчки и доставки, се нареждат сред първите шест най-разпространени стопански престъпления в България, с дял съответно 17% и 15% от всички отчетени случаи на измами.
- 92% от всички анкетирани български участници имат ясно разбиране за риска от компютърни измами, на който са изложени техните организации.

Извършителят и потърпевшият

- Въпреки че компаниите имат повече доверие в своите системи за управление, голяма част от измамите (20%) все още се разкриват по случайност.
- Ролята на оценката на риска от измами е подценена – 35% от анкетираните български компании не са правили подобна оценка.
- Българските участници в проучването демонстрират нулева толерантност към установените вътрешни за организацията извършители – във всички подобни случаи са предприети действия срещу извършителя. Вътрешните извършители са идентифицирани предимно сред средното управленско ниво.
- 55% от отчетените стопански престъпления са извършени от външни за организацията лица, което е индикация, че българските компании не са достатъчно внимателни в процеса си на избор на бизнес партньори.

Измамата – представлява ли тя значителен риск за бизнеса в България?

Нашето проучване показва, че 25% от анкетираните български организации са били обект на измама през последните две години; процент, който е малко под средните показатели за Югоизточна Европа (27%) и за света (37%).

Означава ли това обаче, че стопанската престъпност е по-незначителен проблем в България, отколкото другаде? Отговорът се крие във възможностите на компаниите да идентифицират и отчитат стопански престъпления и – когато рисковете са установени – да предприемат адекватни мерки за противодействие.

Видове стопански престъпления – идентифицирани ли са нови рискове?

Най-разпространените измами

Присвояването на активи е най-често срещаното стопанско престъпление в България (40%), както и в Югоизточна Европа (52%) и в света (69%). Това не е изненадващо, предвид факта че този вид измама е по-лесна за разкриване в сравнение с другите видове стопански престъпления, тъй като става дума за конкретни активи с определена стойност, и дава ясна индикация за това къде мениджърите трябва незабавно да концентрират своето внимание, за да предотвратят подобни загуби.

Счетоводните измами (30%) се нареждат на второ място по разпространение в България, следвани от корупцията (28%). Броят на отчетените случаи на тези два вида измами е значително по-висок, в сравнение с резултатите за Югоизточна Европа и света. По-високото ниво на отчетени счетоводни измами в България (спрямо 22% в Югоизточна Европа и в света) е сигнал, че шест години след началото на глобалната икономическа криза мениджърите все още са под натиск да поддържат определени нива на някои основни показатели за развитие на бизнеса с оглед постигане на определени финансови резултати. Относно корупцията, резултатите от българското проучване (28%) са близки до тези на глобално ниво (27%) и малко по-високи от тези за Югоизточна Европа (23%). Възможно е броят на реално отчетените случаи на корупция да е по-нисък от действителния, тъй като този вид престъпления са труднодоказуеми и често остават неразкрити.

Интересно е също така да се отбележи фактът, че голяма част от ръководителите на различни организации в България считат нелоялната конкуренция за сериозна заплаха, когато става дума за бизнес в световен мащаб (29%). Високата чувствителност към риска от нелоялна конкуренция се оказва характерна черта за целия европейски регион (за 25.3% от участниците от Западна Европа и за 24.5% от тези от Източна Европа), което изглежда е резултат от законодателството на Европейската комисия в тази насока и синхронизирането на местните законодателства с нормите на Европейския съюз. За повече детайли по въпроса, моля вижте глобалния доклад.

Според българските участници най-големите щети, които бизнесът понася в резултат на нелоялна конкуренция, са финансовите загуби (24%) – резултат, идентичен с този за Югоизточна Европа и малко по-висок от този за света (17%). На второ място е уронването на престижа на организациите (18%) – спрямо 22% за Югоизточна Европа и 21% в света.

Нови видове измами

Въпреки че за българските участници компютърните измами и измамите, свързани с поръчки и доставки, са нови категории, тези измами са посочени от тях сред шестте най-често срещани стопански престъпления в България.

За целите на нашето проучване двете категории са дефинирани по следния начин:

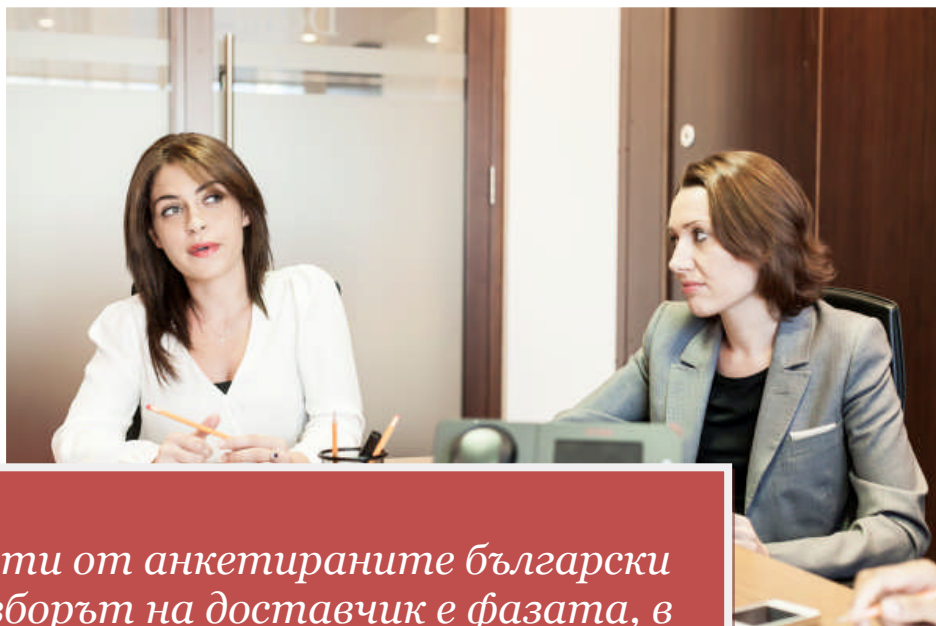
Компютърно престъпление	Измама, свързана с поръчки и доставки
<i>“икономическо престъпление, извършено чрез използване на компютри и интернет. Включва разпространение на вируси, незаконно копиране на файлове, фишинг и фарминг и кражба на лични данни, напр. данни на банкови сметки. Компютърно престъпление има само тогава, когато компютър или компютри и интернет се използват целенасочено, а не случайно”</i>	<i>“незаконно поведение, в резултат на което нарушителят печели предимство, избягва задължение или причинява щета на своята организация. Нарушителят може да е служител, собственик, член на борда, служебно лице (чиновник), публична фигура или клиент, който участва в покупката на услуги, стоки или активи за организацията“</i>

17% от българските участници посочват, че са били обект на компютърна измама през последните две години. Тези резултати са по-ниски от средните за Югоизточна Европа (22%) и за света (24%), но може да се очаква в следващите години случаите на компютърни измами в България да нараснат.

Резултатите показват, че 92% от българските участници в проучването имат ясно разбиране за заплахата от киберпрестъпления, пред която са изправени техните организации.

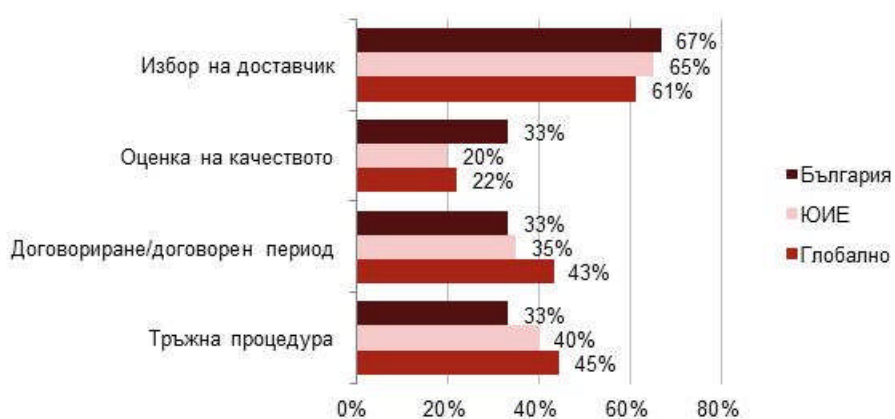
Когато оценяват въздействието на компютърните измами върху своя бизнес, участниците от България посочват кражбата на интелектуална собственост, включително кражбата на данни (38%) и накърняването на репутацията на организацията (37%) като свои основни притеснения. Тези данни са близки до резултатите за Югоизточна Европа и света – съответно кражба на интелектуална собственост – 44% и 36%; и щети върху репутацията – 39% и 41%.

53% от българските участници в проучването възприемат риска от компютърни измами основно като външна заплаха, докато 28% от тях считат, че киберпрестъпленията са както вътрешна, така и външна заплаха за организациите. Само 8% са посочили, че това е изцяло вътрешен риск.



Според две трети от анкетираните български организации изборът на доставчик е фазата, в която най-често се случват измамите, свързани с поръчки и доставки.

Случаи на измами с доставки



ЮИЕ = Югоизточна Европа

Възприемане и реалност – съществува ли разминаване?

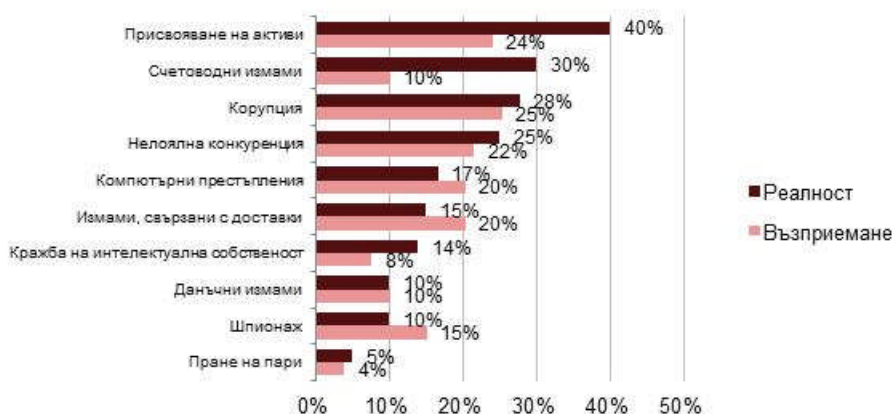
Резултатите от проучването за България показват, че все още съществува разминаване между исторически отчетените случаи на измами и степента на вероятност, според участниците, организациите им да станат обект на подобни измами в бъдеще.

Въпреки факта, че 40% от българските участници са посочили случаи на присвояване на активи през последните две години, само 24% от анкетираните организации в България допускат вероятността тяхната организация да стане жертва на подобна измама в следващите две години.

Още по-голямо е несъответствието между реално отчетените случаи на счетоводни измами и усещането за подобен риск в бъдеще. Това може да е израз на недоверяване, като се има предвид факта, че все още една от всеки пет измами се разкрива случайно или чрез средства, които са извън контрола на мениджърите.

Компютърните измами, измамите, свързани с поръчки и доставки, както и шпионажът са категории, в които усещането за заплахата е по-силно от реалността.

Възприемане срещу реалност



Борбата срещу злоупотребите е непрекъснат процес и организациите не трябва да намаляват своята бдителност, особено като се има предвид, че всеки отделен пазар има различен рисков профил, който се променя динамично във времето в резултат на непрекъснатата поява на нови рискове/заплахи. Въпреки че е невъзможно стопанската престъпност да бъде напълно изкоренена, организациите трябва да продължават да развиват съществуващите и да въвеждат нови системи за контрол, както и да възпитават лоялност у служителите си, с цел изграждане на култура на нетърпимост към злоупотреби, която се налага от висшето ръководство на организациите, т.нар. култура на „добрия пример“.

Цената на измамата – трябва ли да се вземат предвид и „непреките (вторичните) щети“?



25% от организациите в България, които са били обект на стопанско престъпление, са загубили над 100 хил. щатски долара

Измамите нанасят сериозни финансови щети на бизнеса: 25% от организациите в България, които са били обект на стопанско престъпление, са загубили над 100 хил. щатски долара, а други 5% са отчели загуби, надхвърлящи 1 млн. щатски долара.

Към директните загуби трябва да се прибавят и т.нар. „вторични щети“ като накърняване на репутацията на компанията, понижаване на мотивацията у персонала, влошаване на отношенията с регулаторните органи и бизнес партньорите, тъй като те също могат да доведат до загуби за бизнеса: 30% от българските участници в проучването посочват негативния ефект върху мотивацията на служителите като най-значимата непряка щета, която бизнесът им е претърпял през последните две години, вследствие на стопанско престъпление. Еднакъв процент участници (по 15%) посочват влошаването на отношенията с регулаторни органи и с бизнес партньори като най-сериозните индиректни щети за своя бизнес.

Непреки щети

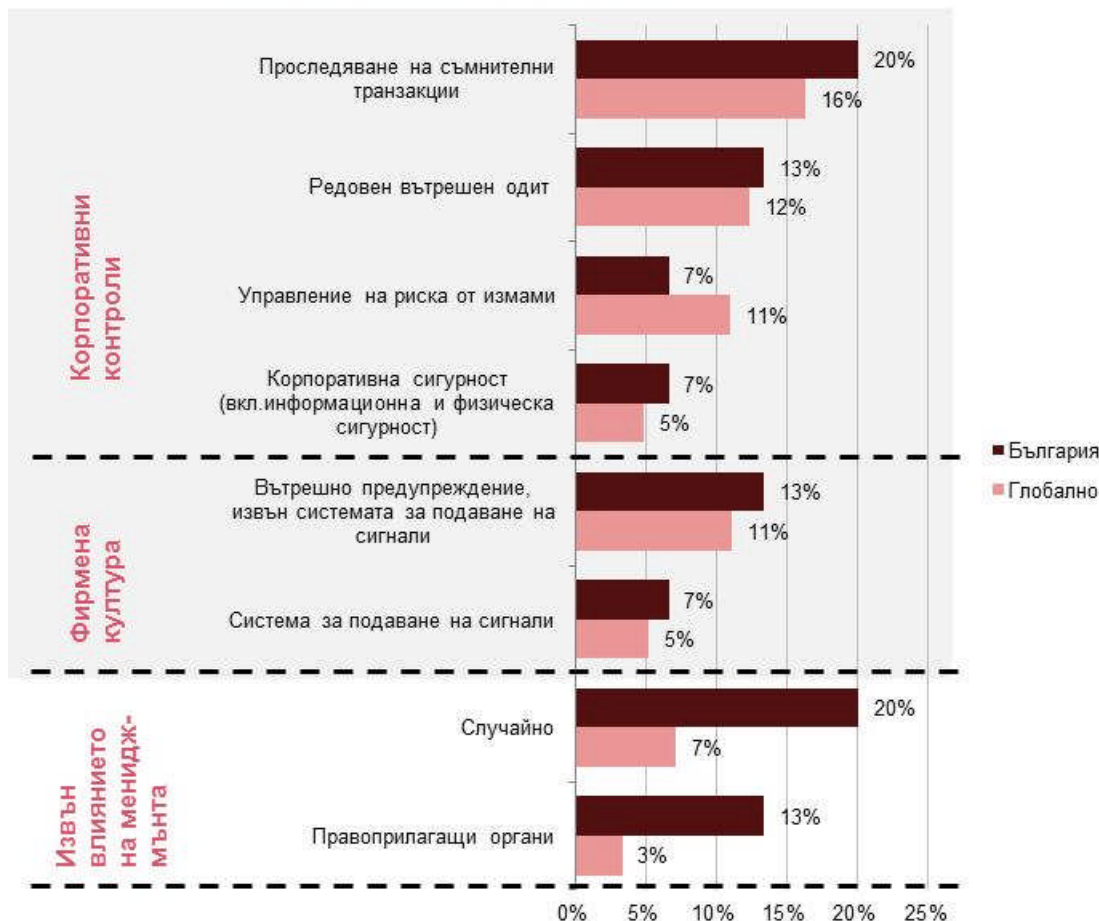


*ЮИЕ = Югоизточна Европа

Разкриване на измами – ефективни ли са средствата за разкриване и предотвратяване на измами?

Методите за разкриване на злоупотреби могат да се разделят на две основни групи: случайно разкриване и разкриване чрез средства, управлявани от мениджмънта, напр. системи за управление на риска и вътрешен одит.

Методи за разкриване на измами



Въпреки факта, че 27% от разкритите измами са разкрити в резултат от ефективно работещи корпоративни контроли като управление на риска от измами или редовни вътрешни одити, една от всеки пет измами все още се разкрива случайно или чрез средства извън контрола и влиянието на мениджмънта. Това е притеснителен знак, който предполага, че в тази област все още има място за подобрене:

- 35% от българските участници посочват, че не са извършвали оценка на риска от измами през последните 24 месеца, като главните причини са или допускането, че това не би имало смисъл (39%), или липсата на разбиране какво точно представлява оценката на риска от измами (18%).
- Само в 7% от отчетените случаи измамата е разкрита чрез механизъм за подаване на сигнали. Този факт е доста изненадващ, тъй като нашият опит показва, че анонимните сигнали помагат на организациите в разкриването на измами, когато други средства за разкриване са се оказали неефективни.

Типичният извършител – познавате ли врага си?

Профилът на типичния извършител в България (подобно на Югоизточна Европа) се различава от профила на глобално ниво, т.е. според 55% от анкетираните български организации (56% за Югоизточна Европа) те са били обект на стопански престъпления, извършени от външни за организацията лица (спрямо 40% на глобално ниво).

36% от българските организации посочват, че външните извършители са били предимно клиенти на компанията, а 27% – че са били техни бизнес посредници. Други 36% посочват категорията „Друг извършител“, която може да включва организирани групи или други индивиди. Този процент е по-висок както от този за Югоизточна Европа (19%), така и от този за света (24%).

Българските организации не са посочили извършители на измами сред заемащите висши управленски позиции, за разлика от участниците от Югоизточна Европа и света. Това предполага, че компаниите са успели да наложат културата на „добрия пример“.

Данните от проучването показват, че ако налагането на правилен тон от мениджмънта е задължително условие, то това съвсем не е достатъчно средство за превенция. Като се има предвид факта, че според данните за България идентифицираните вътрешни извършители са основно на средно управленско ниво (78% спрямо 42% в световен мащаб), изглежда необходимо организациите да увеличат усилията си в посока превенция като добре проучват служителите и мениджърите си преди да ги наемат на работа и редовно правят оценка на ефективността на своите системи. От гледна точка на бизнеса подобни усилия биха стрували по-малко, отколкото справянето с последствията от измами, тъй като превенцията, по правило, винаги е по-евтина, отколкото отстраняването на последствията.

Помолихме участниците в проучването, които са посочили, че са били обект на измами, извършени от вътрешни за организацията лица, да опишат типичния извършител, използвайки следните критерии: възраст, пол, трудов стаж в организацията, образование.

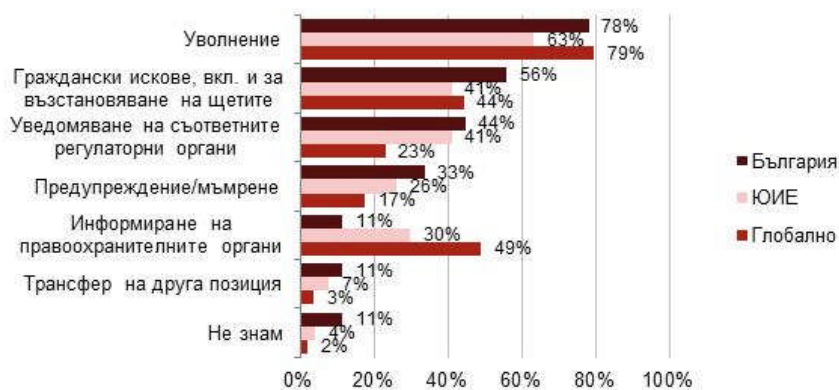
Резултатите за България показват, че типичният вътрешен за организацията извършител е служител на средна възраст с полувисше или висше образование, който е работил за компанията от три до пет години. Тези характеристики са типични за вътрешните извършители и в Югоизточна Европа, и на глобално ниво, но що се отнася до пола на извършителя се наблюдава интересна разлика. Отчетените резултати за България са разпределени поравно между двата пола (по 44.4%); в Югоизточна Европа и на глобално ниво вътрешните извършители са преобладаващо мъже (съответно 63% и 77%). 11.2% от българските участници или не знаят, или са предпочели да не посочват пола на извършителя.

Противодействие спрямо извършителите – важна ли е бързата и адекватна реакция?

След разкриване на дадена злоупотреба е изключително важно организацията да предприеме адекватни действия срещу извършителя, за да се предотвратят други потенциални злоупотреби, както и да се покаже на всички заинтересовани страни, че организацията няма да толерира подобни нарушения.

Нашето проучване показва, че българските организации не се страхуват да предприемат действия срещу извършителите, което е окуражаващ знак.

Действия, предприети срещу вътрешен извършител



Действия, предприети срещу външен извършител



*ЮИЕ = Югоизточна Европа

В случаите, когато извършителят е вътрешно лице, организациите изглеждат по-решени да покажат, че не толерират подобни нарушения, т.е. посочили са, че в такива случаи винаги предприемат действия срещу извършителя. Най-често прилаганата мярка е уволнение на съответния служител (в 78% от случаите), което кореспондира с резултатите за Югоизточна Европа (63%) и света (79%).

Тогава, когато извършителят е външно лице, организациите изглеждат по-предпазливи в действията си спрямо нарушителите – само в 27% от случаите прекратяват бизнес отношенията, докато в 18% от случаите не предприемат никакви действия. Уведомяването на съответните регулаторни или правоохранителните органи са предпочитаните мерки спрямо външните за организацията извършители.

Терминология, използвана в доклада (в азбучен ред)

Законодателство за защита на конкуренцията

Законодателство, което насърчава или поддържа пазарната конкуренция като има за цел да елиминира използваните от организациите нелоялни бизнес практики.

Примери: определяне на цени, дискриминационно ценообразуване, неравноправни търговски условия или обвързване (т.е. купувачът е принуден да закупи и друг продукт, освен този, който желае).

Измама, свързана с поръчки и доставки

Незаконно поведение, с което нарушителят печели предимство, избягва задължение и/или причинява щета на своята организация. Нарушителят може да бъде служител, собственик, член на ръководството, длъжностно лице (чиновник), публична фигура или клиент, който участва в покупката на услуги, стоки или активи.

Компютърно престъпление (Киберпрестъпление)

Компютърно престъпление (киберпрестъпление) е стопанско престъпление, извършено с помощта на компютър и интернет. Типични случаи на компютърни престъпления са разпространяването на вируси, незаконното копиране на файлове, фишинг и фарминг, кражбата на лични данни като банкови сметки, например. В контекста на това проучване компютърното престъпление не включва рутинната измама, при която компютърът се използва като помощно средство за създаване на измамата, а се отнася единствено за такива стопански престъпления, при които компютърът, компютърната мрежа или използването на електронни медии и устройства са основен, а не страничен елемент.

Кражба на интелектуална собственост (включително търговски марки, имитативни продукти и услуги)

Това включва незаконно копиране и/или разпространение на фалшиви стоки в нарушение на патент или авторско право и създаване на фалшиви банкноти и/или монети с намерението да бъдат представени за истински.

Оценка на риска от измами

Оценка на риска от измами се прави, за да се установи дали дадена организация е предприела специфични действия относно:

- Рисквете от измама, на които е изложена организацията;
- Оценка на най-застрашаващите организацията рискове (напр., оценка на рисковете от гледна точка на значимост и вероятност);
- Идентифициране и оценка на съществуващите контроли (ако има такива) за минимизиране на основните рискове;
- Оценка на програми и контроли в организацията за противодействие на злоупотреби; и
- Стъпки/действия за преодоляване на слабости в контролите.

Подкуп и корупция

Незаконното използване на служебно положение с цел получаване на облаги. Това може да бъде обещание за стопанска облага или друга услуга, сплашване или изнудване. Може да се отнася също и до приемането на подобни стимули. Характерни примери: незаконни комисиони, изнудване, обвързващи подаръци, нерегламентирани плащания, и т.н.

Пране на пари

Действия, имащи за цел да узаконят приходите от престъпление, чрез прикриване на реалния им произход.

Присвояване на активи, включително от служители

Кражба на активи (вкл. парични средства, стоки или оборудване) от директори, други служители на отговорни позиции или редови служители с цел набавяне на собствена облага.

Стопанско престъпление/измама

Преднамерено лишаване на друго лице от пари, имущество или законово право чрез нечестни средства.

Счетоводна измама

Финансови отчети и/или други документи са подправени или изготвени по такъв начин, че да не отразяват действителната стойност или финансовите дейности на организацията. Това може да включва счетоводни манипулации, фиктивни заеми/финансиране, подправени

документи за кандидатстване за кредит и неоторизирани транзакции/спекулативна търговия.

Финансова загуба

Включва както преките, така и косвените щети. Преките щети са действителната стойност на загубата, претърпяна вследствие на измамата, а косвените (или „вторичните“) щети обикновено включват разходи, свързани с разследването и разрешаването на проблема, глоби, наложени от регулаторни органи, и/или съдебни разходи. Това изключва разходи, претърпени в резултат от „загуба на бизнес възможност“.

Шпионаж

Шпионажът е действие или практика на шпиониране или на използване на шпиони с цел придобиване на секретна информация.

Контакти за България

Ренета Мамасян

Форензик услуги, България
бул. Мария Луиза № 9-11
1000 София, България
Тел.: +359 2 9355 200
Email: reneta.mamassian@bg.pwc.com

Божидар Нейчев

Старши съдружник Консултантски услуги за
България и Югоизточна Европа
бул. Мария Луиза № 9-11
1000 София, България
Тел.: +359 2 9355 200
Email: bojidar.neytchev@bg.pwc.com

Форензик услуги

Мрежата за форензик услуги на ПрайсуотърхаусКупърс включва форензик счетоводители, икономисти, статистици, бивши служители на регулаторни органи, сертифицирани експерти по разследване на измами и специалисти по форензик технологии. Ние помагаме на организациите да се справят с основните финансови и странични рискове, възникващи в следствие на стопански престъпления. Ние установяваме финансови нередности, анализираме комплексни бизнес казуси, с цел намаляване на бъдещ риск от измами.

PwC оказва съдействие на физически и юридически лица в намирането на ефективни решения за техния бизнес. Ние сме мрежа от фирми в 157 държави с над 184 000 служители, ангажирани в предоставянето на качествени одиторски, данъчни и консултантски услуги. За повече информация, посетете нашия сайт www.pwc.com.

Това проучване се предоставя за обща информация и не представлява професионален съвет. Преди да се предприемат (или да не се предприемат) каквито и да било действия, във връзка с информацията в настоящето проучване, трябва да се потърси професионален съвет. Информацията, съдържаща се в това проучване не се ползва с каквато и да е представителност или гаранция (мълчалива или изрична) за прецизност и пълнота и ПрайсуотърхаусКупърс не носи отговорност за действия (или липса на такива) и техните последици, извършени въз основа на информацията в това проучване, както и за решения, взети въз основа на него.

© 2014 ПрайсуотърхаусКупърс. Всички права запазени. Настоящата публикация не може да се разпространява без разрешение от ПрайсуотърхаусКупърс. "ПрайсуотърхаусКупърс" се отнася за мрежата на ПрайсуотърхаусКупърс Интернешънъл Лимитед (PricewaterhouseCoopers International Limited (PwCIL)) и/или една или повече от фирмите в нея. Всяка от тези фирми е самостоятелно юридическо лице и не действа като агент на PwCIL или на друга фирма от мрежата. PwCIL не предоставя услуги на клиенти. PwCIL не носи отговорност за действия или бездействия на която и да е от фирмите в нейната мрежа, нито може да осъществява контрол върху изпълнението на техните професионални решения или да ги обвърже по какъвто и да е начин. Никоя от фирмите от мрежата не носи отговорност за действие или бездействие на друга фирма от мрежата, нито може да контролира изпълнението на нейните професионални решения или да обвърже по какъвто и да е начин друга фирма от мрежата или PwCIL.