

AKO PLÁVAŤ A NEPOTKNÚŤ SA...

Riziko je problém... alebo?

Marcela Polerecká

Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava
xpolerecka@stuba.sk

Abstrakt. *Rast malej spoločnosti je ako rast malého stromu. Na začiatku si musí zvyknúť na podmienky, v ktorých začal rásť, neskôr sú to klimatické zmeny, rôzni škodcovia a tiež človek. Musí sa naučiť čeliť všetkému... So spoločnosťou je to podobné... s jej rastom, zvyšovaním počtu zamestnancov, vstupovaním do nových, ešte nepreskúmaných projektov, rozširovaním sa, využívaním nových technológií, ale tiež vplyvom ekonomickej a finančnej sféry, sa zvyšuje aj pravdepodobnosť výskytu rôznych rizík. Je veľa spôsobov ako predchádzať rizikám, ako správne plávať a nepotknúť sa. To, čo je potrebné a prvoradé, je správna analýza, naplánovanie všetkých krokov dopredu, určiť pre a proti, čo je potrebné obetovať a čo nie. Pri pohľade na spoločnosť poukazujeme najmä na riziká, chyby a omyly, ktoré vznikajú dôsledkom vplyvu ľudského faktora, nesprávnym postojom, rozhodnutiami, nepremyslenými krokmi a technológiami.*

Kľúčové slová: *rast, riziko, správanie, riešenie problémov, technológie.*

Úvod

Nájsť ten správny čas... To je myšlienka, nad ktorou sa zamýšľa väčšina majiteľov malých či veľkých firiem. Kedy je ten správny čas urobiť krok vpred a zožať úspech a nie pád. A niet sa im ani čo čudovať... V dnešnej dobe plnej obchodných kríz, rivality a snáh ovládnuť voľné miesto na trhu a presadiť sa to nie je vôbec ľahké. Spoločnosti z rôznych odvetví, rôznych veľkostí, každá sa dennodenne stretáva s veľkým množstvom rizík, ktorým musia čeliť.

Každý úspech či neúspech je sprevádzaný aj určitým rizikom. Niekedy je riziko menšie, možno nepatrné, inokedy zas veľké, ohrozujúce a nebezpečné. Pri každom kroku nás čaká kamienok, o ktorý môžeme zakopnúť, ktorý môže spomaliť naše napredovanie.

Do mysle sa mi však vkráda takáto myšlienka: Môže riziko v našom podniku, pri komunikácii s klientmi či zamestnancami, reklame či projektoch spôsobiť aj veľký úspech? Veď každé rozhodnutie je podmienené rizikom. A keby niet rizika, nebol by ani risk a iba ten, kto riskuje, môže dosiahnuť skutočný zisk. Prečo ho teda všetci vnímame tak negatívne? Riziká treba chápať správne. Môžu nám pomôcť, ale aj ublížiť.

Riziko podnikania v akomkoľvek odbore je spojené s existenciou spoločnosti, podniku. Nebezpečenstvo môže mať dvojitý účinok: pozitívny alebo negatívny. Pozitívny vplyv rizík je motivačný, posúva človeka a podnik vpred. Naopak, negatívny vplyv podnik potápa. Najčastejší prejav je strach z neúspechu. Príčiny podnikateľského rizika delíme na dva druhy:

- externé (makroekonomický vývoj, colná a daňová politika, hospodárske a iné krízy, zmeny v legislatíve) a
- interné (vyplývajú z vlastností podnikateľa – podcenenie konkurencie, prílišný optimizmus, nezodpovednosť, slabé technické vybavenie, zlé zabezpečenie systému, a pod.).

Počet dôvodov, prečo dané riziká vznikajú, je neobmedzený. Najčastejšie sa vyskytujú finančné riziká, ktoré sa prejavujú napríklad nedostupnosťou úverov, zvýšenou úrokovou mierou, neúspechom v projektoch, stratou finančného imania. Ďalší typ rizík je technologický: zaostávanie za konkurenciou, neschopnosť zabezpečiť softvérové či hardvérové vybavenie, nesledovanie vývoja a výskumu nových technológií. Medzi rizikami nezaostávajú ani ekonomické a trhové riziká, ktoré sú podmienené cenou konkurencie, ekonomiky a požiadavkami klienta.

Ako sa rizikám vyhýbať a ako ich eliminovať? Vo všeobecnosti je eliminovanie rozdelené do dvoch skupín, teda spôsobov riešenia:

1. ofenzívny spôsob – snažiť sa predísť riziku, delenie rizík a
2. defenzívny spôsob – eliminácia dôsledkov rizík.

V nižšie uvedených podkapitolách poukazujem na príklady jednotlivých rizík, ktoré často nastávajú nielen v malých, ale aj vo veľkých podnikoch.

Technológie

Technologické riešenia tohto storočia významne pomáhajú spoločnostiam vo svojom raste, postupe, ale tiež k predpovedaniu blížiacich sa hrozieb a rizík. Ponúkajú možnosť zakomponovať kontrolu rizík do systému, priamo do kľúčových procesov, a tým zdokonaľiť ochranu a bezpečnosť systému. Práve toto začlenenie do celopodnikových systémov, štruktúr a procesov zohráva veľmi významnú a prídavnú úlohu. Nutnou podmienkou však je, že musí byť dodržaný jednotný postup pri zbere a analýze informácií, musia byť štandardizované a rovnako zoradené do všetkých postupov a štruktúr. Číže musia byť porovnateľné a merateľné. Informačné technológie, nástroje a

softvér sú pre manažment rizík veľmi dôležitou a cennou studňou informácií k predpovediam prichádzajúcich rizík, porúch, kolízií a podobne. Tiež je dôležitá aj vzájomná komunikácia ľudí v jednotlivých štruktúrach systému, ktorá pomáha vyhýbať sa starým chybám a predchádzať ich opakovaniu.

IT nástroje sa zároveň starajú aj o to, aby všetky informácie a samozrejme aj výstupy, boli kontrolovateľné, spätne komentovateľné. Generované reporty musia byť prehľadné a jednoznačné. Je dôležité, aby tieto správy obsahovali potrebné a správne informácie. IT nástroje nahradili manuálne vyhľadávanie v údajoch, pri ktorom vznikalo veľa chýb spôsobených nepresnosťou, ľudským faktorom, alebo boli finančne veľmi náročné.

Spoločnosti by mali hľadať nástroje a technológie, ktoré im pomôžu nielen uľahčiť, ale aj zefektívniť a skvalitniť monitorovanie informácií, reportov, a tým aj zdokonaľiť predpovedanie vzniku rizík a vyvarovanie sa im, prípadne nájsť správne riešenie nápravy.

Nové nepoznané projekty

Každý nový projekt posunie spoločnosť o niečo ďalej, prinesie so sebou niečo nové, nové výzvy, nové skúsenosti. Či už ide o malý alebo o veľký projekt, každý na nás vplýva, učíme sa ním. Netreba sa týchto výziev báť, nezľaknúť sa príležitostí a hľadať možnosti, ako ich využiť. Spoločnosť by mala rásť postupne, každý väčší projekt otvára dvere k ešte väčšiemu projektu, pretože práve tie vyžadujú mať za sebou určité skúsenosti s podobnými projektmi, aj keď v menších rozmeroch. Spoločne s novou výzvou sa k nám však rútia malé aj veľké riziká, problémy, nástrahy, straty, zisk, úspech. Riziká, ktoré sa objavujú pri nových, ešte nepreskúmaných projektoch, sú rôzne.

Hlavným rizikom je nevládnutie projektu, či už ide o nedostatok finančných prostriedkov alebo nedostatok ľudských zdrojov. Významným rizikom je aj neodhadnutie alebo neschopnosť zabezpečenia potrebného softvérového a hardvérového technického vybavenia. Vysoké technické požiadavky projektu nás môžu posunúť ešte do vyššieho rizika, aké sa ukazovalo na začiatku. Spolu s ním prichádza aj nevládnutie požadovanej kvality, prípadne zvyšovanie kvantity na úkor kvality.

Vplyv rizík nesprávneho rozhodnutia a následného nevládnutia projektu je aj strata aktuálnych zákazníkov kvôli nedostatku času. Preto základnou podmienkou je, aby čas, ktorý je zabehnutý pre chod spoločnosti na stále projekty a pre stálych zákazníkov, bol oddelený od času na nové projekty. Pokiaľ nie sme schopní urobiť túto základnú štruktúru, nemáme voľný čas, nie sme pripravení zapojiť sa do nových projektov. Preto si rozdeľme čas a rozhodujme sa bez zbytočného a bolestného rizika.

Nízky dopyt po dostupných službách

Dobre vymyslený plán, stratégia podnikania, ale niekde je problém... Stále málo klientov, zákaziek na služby. V čom môže byť problém? Ako doceliť vyšší obrat?

V dnešnej dobe ekonomickej krízy všetci oveľa opatrnejšie prehodnocujeme investície, využívanie služieb a radšej hľadáme iné, menej bolestivé riešenia. Preto je potrebné okrem dobrých služieb vedieť aj dobre ich predať, posunúť zákazníkov, aby neváhal a oslovil nás. Ale ako sa správne predať? Keď sme malá spoločnosť, je veľká reklama pre nás dobrá?

Podstatou je dostať sa k správne mu zákazníkovi v správnom čase, ponúknuť mu produkt za správnu cenu, na správne miesto a hlavne za účinnej podpory marketingových komunikačných nástrojov. Táto práca je náročná, či už na čas, ale aj na financie. Výsledky prichádzajú neskôr a nikde nemáme zaručené, že práve náš plán, naša reklama nás povedie na popredné priečky. Predtým, ako sa rozhodneme presadiť, je podstatné a dobre rozhodnúť sa, na ktorej časti trhu sa chceme prezentovať. Nesprávny výber oblasti môže mať za následok nielen nulový výsledok, ale aj premrhanie finančných prostriedkov, ktoré sme do marketingu vložili. Marketing je potrebný pre malé aj veľké firmy, aby sme však pri malých firmách predchádzali riziku straty finančných prostriedkov, ktoré vieme využiť úplne inak, na dôležitejšie ciele, je vhodnejší priamy marketing, to znamená oslovenie ľudí priamo, stretnutia, prezentácie. Väčšie spoločnosti sú schopné obetovať balík peňazí na reklamu, či už v televízii, magazínoch alebo na reklamných pútačoch. Zároveň sa však netreba báť investovať a obetovať finančné prostriedky, riziká sú vždy v našej blízkosti, je na nás ako ich zvládame, vyhýbame sa im či zmierňujeme ich následky. V prvom rade je potrebné, aby sme si zvolili tie pravé ciele, za nimi šli a držali sa ich.

Počítačové vírusy, počítačová infiltrácia

Priatelia... Nepriatelia... Každá spoločnosť, fungujúci podnik má svojich priaznivcov, ale aj nepriateľov. Jedného nepriateľa majú spoločného všetky spoločnosti, firmy či informačné systémy. Je ním Vírus. Pán s veľkým V, ktorý každým vývojom technológií, nových softvérov rastie a rastie. Človek by na prvý pohľad povedal, že sa táto otázka netýka spoločností, ktoré sa zaoberajú priamo informačnými technológiami, softvérom či hardvérom. Avšak ani ich toto riziko neobchádza. Sledujeme ako dávajú na prvé miesto práve bezpečnosť. Pravidelne kontrolujú a majú veľké nároky na správne a dôkladne zabezpečenie celého systému. Niekedy však práve finančné otázky posúvajú prioritu zabezpečenia o krok nižšie.

Ako sa proti počítačovým vírusom chrániť? Aký je správny spôsob infiltrácie? Je veľa spôsobov opatrení voči napadnutiu systému vírusom, aby nebolo narušené ani najslabšie miesto v systéme a nevznikla tak trhlina, ktorá bude lákať na zneužitie.

Opatrenia, ktoré nám pomáhajú redukovat', prípadne eliminovať výskyt počítačových vírusov, môžu byť napríklad takéto:

- *Zvýšenie pozornosti pri inštalácii nového softvéru*

Táto problematika sa dotýka v prvom rade softvéru stiahnutého z internetu, je jedno či ide o platený alebo voľne šíriteľný softvér. Softvér je často poskytovaný na stiahnutie z viacerých serverov, tzv. zrkadiel (mirrorov), ktoré majú za úlohu znížiť zaťaženie hlavného servera. Tieto môžu byť kompromitované v prípadoch oboch typov softvérov, preto je potrebné venovať pozornosť kontrolným súčtom, digitálnym podpisom sťahovaných médií, či súhlasia s tými, ktoré sú uvádzané na stránkach výrobcu. V prípade inštalácie zmeneného softvéru sa vystavujeme riziku zneužitia dát uložených na konkrétnom počítači, čo môže viesť k odcudzeniu prístupov na ďalšie počítače v sieti a rozšíreniu vírusu na počítač, kde nebol infikovaný softvér inštalovaný.

- *Určenie primeraných právomocí užívateľom na jednotlivých počítačových staniciach*

Vo väčšine prípadov je používateľ menej skúsený ako administrátor konkrétnej pracovnej stanice, a preto je potrebné eliminovať možnosť spustenia infikovaného softvéru pod účtom s vysokými oprávneniami, čo by malo za následok infikovanie celého systému. Spustenie takého softvéru pod neprivilegovaným účtom by znamenalo v najhoršom prípade infikovanie používateľských dát. Opäť tu je možnosť kompromitácie ostatných systémov, ak sa škodlivý softvér dostane k informáciám o účtoch na okolitých systémoch. Preto sa vo väčšine prípadov ani nedá pod takýmto účtom inštalácia softvéru realizovať.

- *Obmedzenie dostupnosti jednotlivých služieb internetu na jednotlivé počítačové stanice*

Obmedzením dostupnosti služieb len pre počítače, ktoré nutne potrebujú tento prístup a obmedzenie prístupu len na počítače, na ktoré je potrebné mať prístup (napríklad z internetu). Tým docielime zníženie vstupu ľudského faktora, chyby osoby administrátora, ktorý neúmyselne zabudne aktualizovať softvér na všetkých staniciach či serveroch kde sú dané služby spustené a tým by nechtiac umožnil prienik útočníkov do siete, na server.

- *Vhodný typ firewallu zo strany servera k lokálnej sieti*

Firewall je potrebné zvoliť s ohľadom na požiadavky zabezpečenia, miery filtrácie, administrátorského komfortu či využívanie systémových prostriedkov.

- *Zabezpečenie výkonného antivírusového monitoru*

Vírusové skenery, ktoré zabezpečujú monitorovanie každej akcie v systéme, či už prístup zo siete, spustenie softvéru z disku, stiahnutie softvéru z internetu a pod., dokážu zabezpečiť väčšinu vyššie spomínaných situácií.

V dnešnom svete je veľa rizík, ako môže byť systém napadnutý a zavírený. Ako povedal p. Juraj Malcho, ktorý je v spoločnosti ESET vedúci vírusového laboratória: „Väčšina ľudí má pocit, že hacker je niekto, kto je strašne zručný a veľa vie, vo väčšine prípadov to však vôbec nie je pravda. Oveľa jednoduchšie je niečo pokaziť ako opraviť.“[3] A práve preto je potrebné dbať na čo najlepšiu bezpečnosť a chrániť sa voči napadnutiu tohto spoločného nepriateľa.

Porušenie autorských práv inej spoločnosti

Copyright je forma duševného vlastníctva, ktorou dáva autor pôvodného diela výhradné právo na určité časové obdobie, vo vzťahu k tejto práci, vrátane jeho zverejnenia, šírenia a adaptácii. Autorské práva sa vzťahujú na akúkoľvek formu nápadu alebo informácie, ktoré sú podstatné, diskkrétne a stanovené v médiu.

Takto sa prevažne definuje copyright. Ale čo to znamená v skutočnosti?

Autorské právo je na území Slovenskej republiky upravené zákonom č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon). [1] Tento zákon upravuje vzťahy i súvislosti s vytvorením a použitím umeleckého a vedeckého diela, umeleckého výkonu, s výrobou a použitím zvukového a zvukovo-obrazového záznamu, s vysielaním a použitím rozhlasového a televízneho vysielania a v súvislosti so zhotovením a použitím databázy tak, aby boli chránené práva a oprávnené záujmy autora.

Autorské právo vzniká okamihom, keď je dielo vyjadrené v podobe vnímateľnej zmyslami bez ohľadu na jeho podobu, obsah, kvalitu, účel alebo formu jeho vyjadrenia.

Autorské právo sa pritom vzťahuje na dokončené dielo, ale aj na jeho jednotlivé vývojové fázy a časti vrátane názvu diela a mien postáv, ak spĺňajú pojmové znaky diela a sú ako predmety autorského práva v ňom obsiahnuté.

Porušovanie autorských práv v jeho rôznych formách je dnes určite jedným z dominantných foriem porušovania práva i v oblasti informačných technológií.

Najčastejšími formami porušovania autorských práv sú určite nasledovné:

1. *Používanie programov v rozpore s licenčnou zmluvou,*

teda bez platnej licencie, či v rozpore s licenciou, alebo používanie pre viac užívateľov, ako je povolené.

2. *Neoprávnené šírenie počítačových programov,*

duplikovanie médií, ponúkanie možnosti stiahnutia nelegálnych kópií licenčného softvéru, ale aj sprostredkovanie možností peer-to-peer sietí, ktoré umožňujú neautorizovaný prenos programov či iných autorských diel.

3. *Hard disk loading,*

predaj počítačov s predinštalovaným programovým vybavením, spolu s nelegálnou kópiou operačného systému či aplikačných programov v snahe získať si klienta.

4. *Plagiátorstvo,*

tvorba a šírenie počítačových programov, ktoré parazitujú na dobrom mene už zabehnutých produktov kopírovaním ich dizajnu, mena alebo funkčnosti.

Porušenie autorského práva môže byť nepríjemné, nákladné a trestné. [2]

Softvérové pirátstvo

Softvérové pirátstvo a šírenie nelegálneho softvéru prostredníctvom internetu. Jeho tendencia stúpa hlavne v domácnostiach, ale sem-tam sa vyskytuje aj vo firmách. Pirátsky softvér sa darí držať na uzde hlavne firmám, kde sú zavedené dobre fungujúce kontrolné mechanizmy. Často sa však vykrádajú postupy a kódy používané v iných programoch. Na boj proti softvérovému pirátstvu vznikla Business Software Alliance.

Aké sú dôvody softvérového pirátstva?

- Vzhľadom na súčasnú krízu je to aj ňou spôsobený nedostatok financií na zakúpenie legálnych verzií daných softvérov,
- neznalosť právnych dôsledkov, ktoré vyplývajú z používania nelegálneho softvéru,
- ľahké vytváranie kópií,
- rýchly vývoj nových verzií, a s tým spojené následné zvyšujúce sa investície,
- existencia internetových stránok umožňujúcich získať pirátsky softvér...

...tých dôvodov je omnoho viac.

Ale dá sa pred tým aj chrániť? Spôsobov ochrany je viac, no v princípe sa rozlišujú dva typy ochrany:

Softvérová ochrana. V nej sa softvér chráni prístupovým heslom alebo kódom. V druhej vyššej forme tejto ochrany sú náhodne generované čísla, ku ktorým pomocou kľúča, známeho len výrobcovi daného softvéru, bude po zaplattení zaslaný kód, ktorým softvér „odomkne“.

Hardvérová ochrana je považovaná za účinnejšiu. K zakúpenému programu dostaneme aj hardvérový kľúč, ktorý spravidla zasunieme buď do paralelného portu počítača alebo do portu USB, a tým sa program „odomkne“. Ak program skopírujeme a pokúsime sa ho inštalovať na inom počítači, nebude bez kľúča fungovať. Výroba takýchto kľúčov vo veľkých objemoch nie je nákladná.

Špeciálnou formou ochrany je úprava média obsahujúceho daný softvér, takže neumožňuje kopírovanie svojho obsahu. V súčasnosti takmer všetky hry a niektoré hudobné CD nosiče využívajú túto formu ochrany. Otázne je, či výrobcovia sami neporušujú zákon, ak nám bránia vytvoriť si záložnú kópiu pre vlastné potreby.

Keďže väčšina softvérových spoločností nedokáže zistiť na diaľku, či je softvér legálny alebo nelegálny, nezostáva strážcom dodržiavania autorského zákona prakticky nič iné, ako sa spoliehať na udania iných osôb. Spoločnosti BSA ich môžu anonymne poslať priamo cez jej stránku. Najčastejšími „bonzákmi“ sú, povedzme si to na rovinu, rozhnevaní bývalí zamestnanci, ktorí ochotne uvedú počet nelegálnych inštalácií, zoznam nelegálne používaných programov a rôzne iné podrobnosti. Žiaľ BSA tieto akty pomsty podporuje a otvorene vyzýva na anonymné udania ľudí, ktorí ostávajú skrytí a nenesú žiadnu zodpovednosť. BSA aj na základe takto získaných informácií potom väčšinou zašle firme varovný list, prípadne odovzdá informácie orgánom činným v trestnom konaní. [2]

Únik citlivých informácií cez prenosné médium

Rizikom najmä veľkých a prosperujúcich firiem je únik citlivých informácií. Čo pod tým presne myslíme?

Spoločnosť vyvíja softvér, ktorý bude novinkou na trhu. Bude to veľký BOOM a spoločnosť získa popredné priečky na trhu. Otázkou však je ľudský faktor – človek, ktorý vo vidine možného zisku zapredá svoju dôveru materskej spoločnosti a získa citlivé informácie o projekte pre konkurenciu. Nielenže zlyhal ako človek, ale spoločnosť pripravil o možný zisk, slávu a miesto na trhu.

Ako sa proti takémuto prípadu brániť? Je to veľmi náročné. Správny výber zamestnancov, podpísanie zmlúv o dôvere a mlčanlivosti, zapojenie technológie. Vo veľkých firmách tento problém riešia zakázaním komunikácie cez e-maily, rôznych komunikačných klientov, ako sú napríklad icq, msn, gtalk okrem internej komunikácie a e-mailov, ktoré sú posielané z firemnej a kontrolovateľnej adresy. Ďalší spôsob ochrany je napríklad zablokovanie USB portov, počítačové zostavy bez napaľovačiek, ktoré rušia možnosť nakopírovania dát na prenosné médium a ich úniku mimo brán spoločnosti.

Aj keď sú možnosti ako zabrániť strate cenných informácií a dalo by sa ísť až do „chorobnej“ hĺbky, spoločnosť musí dôverovať svojmu zamestnancovi, čo však neznamená bezhraničnú dôveru. Rovnako aj zamestnanec je povinný dodržiavať pravidlá a nesklamať

dôveru spoločnosti. Je potrebné, aby boli dodržiavané morálne pravidlá, sme predsa ľudia a nie roboti naprogramovaní na vidinu peňazí.

Záver

Na záver by sme sa chceli zamyslieť nad niečím, čomu sme doposiaľ v práci nevenovali priestor, ale čo považujeme za rovnako dôležité ako všetky ostatné faktory. Šťastie. Myslím si, že niekedy aj ono zohráva dôležitú úlohu, hlavne pri začínaní akéhokoľvek projektu či rozrastaní sa podniku. Akokoľvek sa môže podnikateľ snažiť, nikdy sa mu nepodariť zväziť úplne všetky riziká, odhadnúť každé úsilie či vymyslieť dokonalú stratégiu.

Verím však, že plánovaním sa dá väčšine problémov predísť. Potom si už len treba veriť a ísť za svojím cieľom, za snom vytvoriť niečo produktívne, kreatívne a úspešné. Niečo, čo zaujme druhých, niečo, čo pomôže zlepšiť informačný systém a pritom niečo, čo je schopné odolávať prichádzajúcim rizikám či krízam. Verím, že aj Šťastena sa na začínajúcich podnikateľov občas usmeje.

Použitá literatúra

1. Gregušová, D., Chápala, M., Susko, B.: Autorskoprávna ochrana počítačových programov na Slovensku. Dostupné na stránke: <http://www.epi.sk/Main/Default.aspx?Template=/Main/TArticles.ascx&phContent=/Main/ArticleShow.ascx&ArtID=6648&LngID=0&CatID=66>
2. Oster, J.: Porušovanie práv duševného vlastníctva. Dostupné na stránke: http://www.zodpovedne.sk/kapitola3.php?cl=autorske_prava
3. Ulej, T.: Ako sa chytajú počítačové vírusy. Dostupné na stránke: <http://pocitace.sme.sk/c/4101345/ako-sa-chytaju-pocitacove-virusy.html> (1. 10. 2008.)

Annotation

How to swim right and walk straight.

There are parallels between the growth of a small company and that of a tree. Confronted with the necessity of getting used to the conditions and particular surroundings in the first place, the tree later becomes faced with climatic changes, pest infestation and, last but not least; the man. It has to learn to hold up no matter what... As for a company, the process is rather similar... Its growing, taking on new staff, launching new and unexplored projects, expanding, exploiting new technology, but also the impact of economic and financial fields result in increased occurrence of risks. There are many ways of how to prevent risks or, let us say, how to swim right and walk straight. The correct analysis and point-by-point planning ahead, defining pros and cons as well as making the right sacrifices, are company's thorough necessities and priorities to follow. When analysing the society, we most often point out the risks, mistakes and missteps that are caused by human factor, by having the wrong approach and taking the wrong decisions, or else, that are due to technology and ill-considered moves.