

Ako sa nebát'?

IGOR JÁNOŠ

*Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava
janos@radlight.com*

Abstrakt. Minimalizácia šance neúspechu je jedným z najdôležitejších cieľov každého manažéra nie len softvérového projektu. Je nutné si uvedomiť hrozby, ktoré projektu hrozia v každej jeho fáze a určiť kroky, ktorými je možné sa hrozbám vyhnúť, alebo aspoň minimalizovať ich negatívne dopady na úspech projektu. Mnoho projektov končí neúspechom, čo je znakom toho, že manažmentu rizík sa v dnešnej dobe stále nevenuje dostatočnej pozornosti v mnohých firmách.

V tejto práci skúsím priblížiť postupy, ktoré sa dnes v praxi používajú na analýzu, plánovanie a minimalizáciu rizík hroziacich pri vývoji softvéru a skúsím ich konfrontovať s mojimi skúsenosťami s prácou na menších projektoch v malom tíme.

Úvod

Napriek tomu, že som mladý, som mal skúsenosť s prácou na viacerých projektoch pre domáce aj zahraničné firmy. Hoci jednotlivé komponenty, ktoré sme vypracovávali, boli zvyčajne samostatne načas dokončené a funkčné, z výsledných systémov veľmi často nebolo nič. Tento fakt dokazuje, že manažmentu rizík sa stále nevenuje dostatočnej pozornosti [2]. Samotní vývojári bývajú veľmi optimistickí vo svojej povahe a neradi robia detailné plány jednak z dôvodu čistej lenivosti, ale aj preto, lebo pri vývoji softvéru prichádzajú vždy prekvapenia. Z mojich skúseností môžem povedať, že každé prekvapenie bude viac alebo menej zlé.

Riziko

Riziko je niečo zlé, čo sa ešte nestalo. Boli by sme veľmi radi, keby to takto aj zostalo, ale nie vždy to býva pravda. Riziko je udalosť, ktorá môže mať negatívny dopad na náš projekt. Dokáže ovplyvniť úplne všetko, čo súvisí s naším projektom. Nešťastná udalosť môže drasticky zvýšiť výrobné náklady. Ak nám konkurencia odláka

najdôležitejších pracovníkov, alebo zhorí pracovná budova, je celkom možné, že náš projekt zanikne úplne. Spravidla najviac náš môžu ohroziť také hrozby, o ktorých nevieme. Je preto veľmi dôležité si uvedomovať zraniteľnosť a primeraným spôsobom sa k nej postaviť – najlepšie jasným a systematickým spôsobom.

Rozdiel medzi problémom a rizikom je veľmi jednoduchý. Problém je situácia, ktorá už nastala a vyžaduje našu okamžitú pozornosť a čo najrýchlejšie jednanie. Riziko je niečo, na čo sa môžeme dôkladne pripraviť. Existuje viacero spôsobov, ako sa vysporiadať s rizikom. Môžeme proste prijať myšlienku na to, že sme zraniteľní a dúfať, že to nejako prežijeme – takýto pštrosí prístup nebýva veľmi šťastné riešenie spravidla pri väčších projektoch. Môžeme jednoduchým spôsobom spísať zoznam hrozieb, strát, ktoré by sme mohli utrpieť a krokov, ako sa im vyhnúť. Tiež môžeme veľmi systematicky a pedantne postupovať podľa praxou overených postupov a minimalizovať tak riziko zlyhania projektu.

Spravidla býva rozdiel medzi tým, ako rôzne riziká vnímajú vývojári a manažéri. Vývojári ako ja bývajú veľmi optimistickí a každý problém berú ako výzvu a skúšku svojich schopností, ktorým tak veľmi dôverujú. A preto bývajú často pri odhadoch až príliš optimistickí. Manažéri naopak často veci vidia až príliš čierne, ale častejšie mávajú pravdu. Je naivné sa spoliehať, že sa nič zlé nestane, ak sa stať môže a plány, ktoré neobsahujú aj katastrofické scenáre sa viac hodia do rozprávok ako do skutočného sveta.

Dá sa niečo robiť?

Ak sa snažíme manažovať riziká formálnym spôsobom, poskytujeme sebe a aj celému tímu veľkú výhodu. Máme v rukách spôsob, ktorým sa dá reálne brániť možným hrozbám. Môžeme tímovo spolupracovať na identifikácii rizík. Postupná identifikácia rizík, určenie šance ich naplnenia, stanovenie možných strát a odhadnutie protiopatrení je možné uchovávať, porovnávať a ďalej rozširovať. Musíme si uvedomiť, že tak, ako sa vyvíja produkt, sa vyvíjajú aj hrozby a že manažment rizík nie je jednorázový krok. Preto je výhodné si všetky informácie ohľadom hrozieb uchovávať a periodicky obnovovať.

Čo všetko sa môže stať?

Odpoveď na túto otázku nepozná nikto, ale ak opakovane hľadáme hrozby pre každý projekt, zistíme, že sa často opakujú. Pre podobné projekty s podobným rozsahom existujú aj veľmi podobné riziká. Preto, ak urobíme dôkladnú analýzu rizík pre jeden projekt, môžeme zvýšiť naše šance aj v budúcnosti. Na nešťastie je zoznam hrozieb taký dlhý, že nikdy si nebudeme úplne istí, že sa nám všetko podarí. Preto by sme nikdy nemali hovoriť, že sa nič nemôže stať, alebo že projekt bude zaručene úspešný. Všetko je iba o zmenšovaní pravdepodobnosti neúspechu... a samozrejme to stojí peniaze.

Musíme sa jasne zamyslieť, do akej miery je pre nás nutné sa venovať manažmentu rizík, hoci ide o veľmi dôležitú činnosť. Je každému jasné, že pre projekt, na ktorom pracujú dva mesiace dvaja ľudia asi nebude potrebovať celú divíziu bezpečnostných manažérov. A asi je každému jasné, že projekt pre 500 ľudí na 5 rokov práce bez plánovania rizík nemá veľkú šancu prežiť. Kedy, čo robiť nám nepovie nikto – cit pre odhad získame až praxou.

Typické softvérové hrozby

Ako som už spomenul, zoznam vecí, ktoré sa môžu prihodiť je nekonečne dlhý. Niektoré sa však objavujú častejšie. Capers Jones identifikoval päť najvýraznejších hrozieb, ktoré ohrozujú softvérové projekty v rôznych sektoroch použitia [3]. Znázorňuje ich tabuľka 1.

Sektor	Rizikový faktor	Percento ohrozených projektov
Informačné systémy pre manažment	Obmedzenie používateľských požiadaviek	80 %
	Prívelký tlak plánov	65 %
	Nízka kvalita	60 %
	Prekročenie nákladov	55 %
	Nedostatočné možnosti nastavení	50 %
Komerčný sektor	Nedostatočná používateľská dokumentácia	70 %
	Nízka spokojnosť používateľa	55 %
	Prídlhý čas na uvedenie do predaja	50 %
	Záškodnické činy konkurencie	45 %
	Súdne trovy	30 %

Tab. 1. Najvýraznejšie hrozby podľa Jonesa

Karl Wiegers vo svojom článku [5] ďalej uvádza ďalšie možné problémy, z ktorých niektoré môžeme ovplyvniť iba nepriamo. Tieto riziká vznikajú kvôli vonkajším faktorom alebo tretím stranám. Môže sa jednať napríklad o vzťahy našich subdodávateľských firiem, položky alebo informácie, ktoré má na starosti zákazník, vzájomné závislosti pracovných skupín, alebo dostupnosť dostatočne skúsených ľudí.

Čo všetko treba ustriehnuť?

Projekty si na svoje úspešné ukončenie samé kladú množstvo požiadaviek, ktoré musíme byť schopní zabezpečiť. Aj keď v počiatočných fázach projektu si môžeme dovoliť tolerovať určitú mieru neistoty, nesmieme tieto požiadavky podceňovať a musíme sa sústrediť a ustriehnuť si tieto faktory :

- nedostatok jasnej vízie budúcnosti
- nerozlišovanie dôležitosti požiadaviek
- nový trh s neurčitými potrebami
- nové aplikácie s neurčitými požiadavkami
- rýchlo sa meniace prostredie
- nedostatočne špecifikované produktové požiadavky

Posledný menovaný faktor sa dá vtipne ilustrovať známou scénkou o sluhovi a pánovi.

Pán: „Potrebujem kameň.“

Sluha: „Áno pane.“

...o chvíľu neskôr...

Sluha: „Tu je váš kameň, pane.“

Pán: „Ten kameň je nepoužiteľný, potrebujem poriadne veľký kameň.“

...o ďalšiu chvíľu neskôr...

Sluha: „Pane, tu máte nový kameň.“

Pán: „Tento predsa nemôžem použiť. Je príliš drsný, potrebujem hladký.“

...o ďalšiu chvíľu neskôr...

Sluha: [odfukujúc] „Hladký veľký kameň, pane.“

Pán: „Prečo si priniesol hnedý kameň? Tie predtým boli čierne. Zožeň mi čierny kameň.“

Je zaujímavé, že nie vždy je možné povedať, kto urobil chybu. Ak zadávateľ a vývojár nepracujú v rovnakej oblasti, často sa stáva, že používajú rozdielnu terminológiu alebo si vôbec nerozumejú. Býva rovnako ťažké pre zadávateľa vyjadriť, čo skutočne potrebuje ako pre vývojára pochopiť, čo sa mu zadávateľ snaží vysvetliť.

Chyby však môžu robiť aj priamo manažéri. Projektoví manažéri bývajú často tými ľuďmi, ktorí vypracúvajú aj plány rizík a keďže každý radšej hľadá chyby a problémy mimo seba, bývajú riziká týkajúce sa manažmentu často podceňované až ignorované. Ak si nedáme pozor na hrozby také, ako tu uvádzam, môžeme sa ľahko dostať do problémov.

- nedostatočné plánovanie a zadávanie úloh
- nedostatočná možnosť viditeľnosti stavu projektu

- nejasné určenie kompetencií a rozhodovania
- nereleastické rozhodnutia
- prestrelené očakávania
- osobné konflikty zamestnancov
- nedostatočná komunikácia

Akú úlohu hrajú informácie?

Nedostatok informácií býva veľmi dôležitým faktorom. Stáva sa, že kým zápasíme so zdanlivo nevyriešiteľným problémom, objaví sa informácia, ktorá pomôže problém vyriešiť úplne iným spôsobom a podľa Murphyho zákonov sa tá informácia objaví u konkurenčnej firmy vždy skôr ako v našej. Je preto dôležité, aby manažér mal prehľad o tom, čo sa deje v blízkom okolí a aj vo svete. Informácie sú kľúčové aj v samotných pracovných skupinách. Je pre nás veľkou výhodou mať výborne vyškolený a skúsený tím ľudí, ktorí rozumejú technikám, postupom a aj prostriedkom, ktoré majú na prácu používať. Ľudí by sme si mali tiež voliť tak, aby rozumeli problematike, ktorú chceme našim projektom riešiť a vyberať si napríklad ekonomicky vzdelaných ľudí, na riešenie systému pre podporu finančného oddelenia firmy. Ku kvalitným informáciám počítame aj podrobnú dokumentáciu, ktorá je vyžadovaná aj zákazníkom, ale je veľmi dobré ju písať aj kvôli interným potrebám. Stáva sa, že sa zamestnanci vo firme menia a potom býva ťažké nájsť a opraviť možnú chybu v programe.

Sú nejaké overené postupy?

McConnel vo svojej práci [4] identifikoval päť prístupov ako sa vysporiadať s hrozbami. Krízový manažment je reakcia na neidentifikované riziko, ktoré sa vyvinulo do aktuálneho nebezpečenstva. Iba mierne lepšie riešenie je poopraviť produkt, keď sa zistí zlyhanie. Aktívny prístup identifikuje riziká, ktoré ohrozujú náš projekt a plánuje, ako im čeliť. Ešte lepšie je podniknúť akcie, ktoré zabránia, aby mohla daná hrozba v budúcnosti niekedy ohroziť náš projekt. Najlepšie riešenie je odstrániť príčiny vedúce k tomu, aby konkrétne hrozby mohli opakovanne ohrozovať náš projekt.

Pod manažmentom rizík rozumieme aplikáciu vhodných nástrojov a krokov za účelom udržania rizík v prijateľných limitoch. Manažment rizík sa skladá z niekoľkých podčastí.

1. Odhadnutie rizika je proces skúmania a identifikácie oblastí, ktoré sú zraniteľné hrozbám. Identifikácia rizík môže byť uľahčená jednoduchým zoznamom bežných oblastí, ktoré sú známe pre

softvérové projekty, alebo analýzou identifikovaných rizík pri predchádzajúcich projektoch. Analýza rizík zahŕňa aj skúmanie, ako sa výdavky na projekt zmenia pri zmene vstupných hodnôt rizík.

2. Rozdelenie rizík je pre náš projekt veľmi dôležité. Určujeme pri ňom, do akej miery je pre nás hrozba nebezpečná, aké sú jej dôsledky a pomáha nám stanoviť, na ktoré riziká sa máme zamerať viac a na ktoré menej.
3. Vyhnutie sa riziku je jednoduchá metóda, ako nič nepokaziť. Ak je to nebezpečné, proste to neurobíme. Ak máme vyskúšanú metódu, radšej použijeme tú a nebudeme hazardovať s novou neodskúšanou.
4. Kontrola rizík zahŕňa plánovanie, riešenie a monitorovanie hrozieb. Zistíme pri nej, ako sa máme chovať, ak nastane daný problém a môžeme sledovať, ako sa jednotlivé hrozby vyvíjajú.

Riziká si môžeme zapisovať do formulárov [5], ktoré nám pomáhajú jednak vizualizovať jednotlivé náležitosti a hlavne umožňujú formálny prístup k celej problematike. Takto uchované riziká môžeme archivovať, a sledovať ich vývoj v čase. Hovorí zrozumiteľnou rečou pre takmer každého.

ID: <i>Identifikačné číslo</i>	Klasifikácia:	Dátum nahlásenia: <i>Kedy bola hrozba nahlásená</i>
Popis: <i>Popíšeme každú hrozbu vo forme „podmienka – dôsledok“</i>		
Pravdepodobnosť: <i>Aký je šanca, že sa z hrozby stane problém?</i>	Dopad: <i>Aký je dopad, ak sa z hrozby stane problém</i>	Vystavenie: <i>pravdepodobnosť x straty</i>
Prvý indikátor: <i>Popíšeme, čo sa dá chápať ako prvý indikátor nadchádzajúceho problému</i>		
Postup zmiernenia: <i>Zadáme jeden alebo viacero postupov, ktoré je možné vykonať na zmiernenie pravdepodobnosti hrozby.</i>		
Dátum začiatku: <i>Dátum, kedy sa začal implementovať plán zmiernenia</i>	Dátum dokončenia: <i>Dátum, dokedy má byť plán zmiernenia hotový</i>	Zodpovedná osoba <i>Priradíme každej hrozbe osobu zodpovednú za vyriešenie hrozby</i>
Aktuálny stav: <i>Popíšeme momentálny stav a účinnosť krokov zmiernenia dopadu k dátumu písania tejto správy.</i>		
Výnimočný plán: <i>Popíšeme, aké kroky sa majú vykonať, ak sa z hrozby stane skutočný problém.</i>		
Podmienky na spustenie výnimočného plánu: <i>Zadáme, kedy sa majú vykonať kroky výnimočného plánu.</i>		

Tab. 2. Formulár na evidenciu rizík

Záver

Myslím, že nakoniec nie je boj s hrozbami taký nerovný, ako sa spočiatku zdalo. Systematickým prístupom a rokmi praxe sa takmer každý manažér môže naučiť ako hrozbám čaliť a dobre ich zvládať. Priekopníci softvérového inžinierstva už problematiku kontroly rizík rozvinuli na takmer plnohodnotnú vednú disciplínu, takže je len na nás, koľko si z nej dokážeme vziať a koľko jej zas chceme vrátiť ako odkaz pre budúce generácie softvérových manažérov.

Použitá literatura

1. Boehm, Barry W. *Software Risk Management*. Los Alamitos, Calif.: IEEE Computer Society Press, 1989.
2. Jones, Capers. *Software Project Management In The Twenty-First Century*. 1999
<http://www.spr.com/news/SoftwareProjectArticle.pdf>
3. Jones, Capers. *Assessment and Control of Software Risks*. Englewood Cliffs, N.J.: PTR Prentice-Hall, 1994
4. McConnel, Steve. *Rapid Development: Taming Wild Software Schedules*. Redmond, Wash: Microsoft Press, 1996.
5. Karl E. Wiegers. *Know Your Enemy: Software Risk Management*. Software Development magazine, 1998
http://www.processimpact.com/articles/risk_mgmt.html

Annotation

How not to be afraid?

Minimizing the failure probability is one of the most ultimate goals of every manager. It is important to realize the risks that can endanger our project in every stage and to estimate countermeasures that can avoid the risks or at least minimize the negative effects on our project's success. Many projects still fail and make obvious one fact – that risk management is not taken seriously by many companies nowadays.

In this essay I will try to describe several ways of managing risks that are being widely used today to analyze, plan and control risks. I will try to express my experiences with work on smaller projects in smaller teams.