Nejčastější chyby v *oblasti Disaster Recovery a Business Continuity Managementu*

Vladimír Kufner

Hewlett-Packard
Vyskočilova 1/1410, 140 21 Praha 4
Vladimír.kufner@hp.com

Abstrakt: *Článek klade za cíl zaměřit se na některé nejčastější chyby v oblasti Disaster Recovery/DR a Business Continuity Managementu/BCM jak na straně útvaru IT, tak i businessu. Dále představuje trendy v oblasti DR/BCM a navrhuje možná řešení založené na praxi autora. Kromě doporučení se zde uvádí i některé reálné příklady z praxe.*

Abstract: *The article focuses on the most common mistakes in the area of Disaster Recovery/DR or Business Continuity Management/BCM, both at IT department side and side of the business. Article introduces some latest trends in the area of DR/BCM and suggests possible solution of the previously mentioned mistakes base on author's experience. Apart of some recommendation are here discussed also the real life examples..*

Klíčová slova: ITIL, ISO, Disaster Recovery, Business Kontinuity Management, Enterprise Risk Management, High Availability, CRAMM

Keywords: ITIL, ISO, Disaster Recovery, Business Kontinuity Management, Enterprise Risk Management, High Availability, CRAMM

1. Úvod

Obnova po havárii neboli Distaster Recovery/DR či dokonce plánování kontinuity obchodních procesů (Business Continuity/BC) je ve většině organizací vnímána jako velmi náročná činnost a to jak z pohledu nutných zdrojů, tak i času a vynaložených nákladů. Velmi často se stává, že se tato činnost podceňuje a nebo se provádí pouze formálně. Pokud jde o situaci, že dokonce ani strana businessu se o tyto věci nikterak nestará, odsouvá se DR v pomyslném žebříčku priorit IT někam hodně dozadu. To může být vzhledem k reaktivní orientaci (*firefighting*) typických oddělení IT někdy velmi nebezpečné.

1.1 Mezinárodní a lokální normy

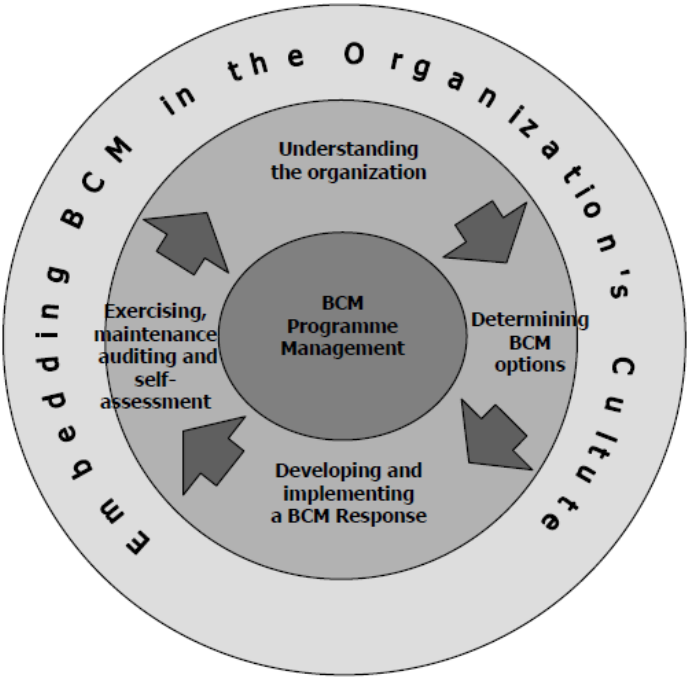
Pro oblast DR/BC existuje celá řada mezinárodních norem či regulativů. Např. ve Spojených státech a Kanadě je to norma NFPA 1600 ([4]), HB221 a APS 232 v Austrálii a FSA (UK). Kromě norem jsou to ještě doporučení pro BC/DR – např. vydávaná americkou burzou – NYSE Rule 4370. Pro účely tohoto článku zůstaneme hlavně u mezinárodních standardů řady ISO. Důvodem je skutečnost, že tyto standardy více odráží principielní věci a nejde tak o regulativní legislativu jak je tomu např. Ve Spojených státech[1].

[1] Zde se významně projevuje rozdíl v právech mezi USA, UK a kontinentální Evropou a ostatním světem, kde se v prvním případě uplatňuje koncept „*law by rule*" (typicky např. Sarbanes-Oxley) a nikoliv „*law by principle*" jako třeba u řady norem ISO.

1.1.1 BS 25999

BS 25999 je britská norma vydaná britským institutem pro normalizaci BSI stejně jako řada dalších standardů kvality. V tomto konkrétním případě je o problematiku v oblasti Business Continuity Management (BCM). Tato norma nahrazuje PAS 56 (*Publicly Available Specification*), uveřejněnou v r. 2003 na stejné téma.

První část "*BS 25999-1:2006 Business Continuity Management. Code of Practice*", vydaná v r. 2006, shrnuje obecný návod jak ustanovit procesy, definuje základní principy a terminologii pro BCM, koncept vytvoření Business Continuity Management Systém/BCMS, programový management, určení variant ochrany pro BCM, vývojem a implementací opatření v oblasti BCM a v neposlední řadě zabudování BCM do kultury organizace.



Druhá část "*BS 25999-2:2007 Specification for Business Continuity Management*", publikovaná v r. 2007, určuje požadavky na implementaci, provoz a zlepšování a dokumentovaný Business Continuity Management System (BCMS), popisující pouze požadavky, které lze objektivně a nezávisle auditovat.

1.2 ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management

Další normou v této oblasti směřovanou spíše do oblasti veřejných služeb je tento mezinárodní standard. Termínem „Incident“ se zde rozumí spíše něco jako havárie datového centra, nikoliv ve významu ITIL procesu Incident management. Norma mající

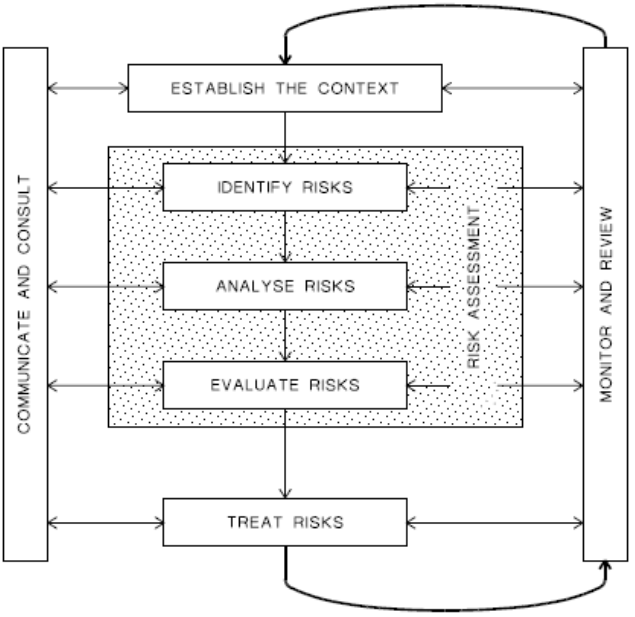
kolem 30 stran používá poněkud odlišnou terminologii než třeba ITIL a směřuje do oblasti společenské bezpečnosti. Stejně jako ostatní standardy kvality ISO používá Demingův cyklus.

1.3 ISO/IEC 24762:2008 . Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services

Jedná se o standard vysloveně pro oblast DR v oblasti služeb ICT aplikovatelný jak pro služby, tak i fyzická zařízení ať již provozované interně či outsourcované. Obsahuje rámcový přístup k DR, včetně vazeb na rizika a bezpečnost (norma řady 27001). Poměrně rozsáhlá norma, v tuto chvíli rozsáhlejší (67 stran) a podrobnější ve svém záběru než třeba ITIL. Vychází z původní Singapurské normy.

1.3.1 AS/NZS 4360 Standard in Risk Management

Jedná se o australskou a novozélandskou normu v oblasti správy rizik. Tato norma definuje základní termíny a definuje procesní rámec – viz následující obrázek.



1.4 Definice některých klíčových termínů

Jelikož v reálné praxi se některé termíny trochu interpretují jinak v různých firmách, pokusil jsem se zde shromáždit nejobvyklejší definice, vysvětlení a interpretace obvyklé na trhu. V potaz jsem přitom bral jednak definice z Wikipedie, dále definice ze standardu ITIL a v neposlední řadě definice používané v auditorské branži.

1.4.1 Wikipedia

Disaster Recovery/DR

Jde o proces, politiky a procedury, které jsou vztaženy k přípravě obnovy nebo zajištění kontinuity technické infrastruktury kritické pro organizaci po přírodních či lidmi zapříčiněných katastrofách. DR je podmnožinou business kontinuity/BC. Zatímco BC zahrnuje plánování udržení všech aspektů obchodních procesů v době ničivých událostí, DR se koncentruje na IT nebo technické systémy, které podporují obchodní funkce.

Business Continuity Management/BCM

Business continuity je aktivita, pomocí které organizace zajišťuje, že kritické podnikové funkce (funkce businessu) budou dostupné zákazníkům, dodavatelům, regulátorům a dalším stranám, které musí mít k těmto funkcím přístup. Tyto aktivity zahrnují mnoho činností prováděných na denní bázi jako je projektové řízení, provádění zálohování, změnové řízení a Service Desk. Business Continuity není nic, co by se mělo implementovat v čase havárie nebo nějaké katastrofy; Business Continuity se odkazuje na aktivity prováděné na denní bázi – zaměřené na údržbu podnikových procesů (business služeb) a jejich konsistenci a obnovitelnost.

Základem BC jsou standardy (směrnice), vývojový program a podpůrné politiky, návody a procedury nutné k zajištění toho, že firma může pokračovat v poskytování služeb v případě nějaké události bez ohledu na její charakter a negativní aspekty. Veškerý návrh systémů, implementace, podpora a údržba by měly být založeny na základě BC, DR a v některých případech systémové podpory. BC je někdy mylně zaměňována s DR, ale jedná se o 2 separátní entity[2]. Zpravidla říkáme, že DR je subset BC.

Termín BC popisuje mentalitu nebo metodiku provádění dennodenních aktivit businessu, zatímco termín *Business Continuity Planning*[3] je aktivitou určující jaká metodika by to mohla být. Plán na BC je potom ztělesněním této metodiky – je určen pro každého ve firmě k provádění běžných provozních operací.

Enterprise Risk Management/ERM

Termín, který se zabývá správou a řízení rizik na úrovni korporace. Jedná se o disciplínu, při které organizace v různých sektorech průmyslu provádějí odhad, řídí, využívají, financují a monitorují rizika pocházející z různých zdrojů za účelem zvyšování krátkodobé a dlouhodobé hodnoty vůči svým akcionářům a dalším zúčastněným stranám.

U zrodu jak termínu, tak i rámcového modelu *stojí Committee of Sponsoring Organizations of the Treadway Commission* (COSO) [2] a *American Institute of Certified Public Accountants* [3].

Samotný termín Riziko se zde vnímá nejenom jako možné ohrožení, ale také jako příležitost v podnikání na volném trhu. Operuje se zde také s termínem portfolio, kdy se jednotlivá rizika v portfoliu prostě nesčítají, ale je nutné počítat s efektem jejich integrace a vzájemné provázanosti.

Je nutné zdůraznit, že ERM zahrnuje celou řadu analytických, statistických metod, jak provádět kalkulace rizik, takže se jedná o dnes velmi propracovanou disciplinu, která logicky doplňuje oblast BC/DR.

[2] či lépe řešeno systémové a procesní pohledy

[3] Dle ITIL a BS 25999 Business Continuity Management.

Součástí a nebo spíše podmnožinou ERM je BIA. ERM se tedy koncentruje na širší záběr rizik než samotná BIA.

Možný způsob provádění ERM v kontextu procesních toků je zvýrazněn na následujícím obrázku.

1.4.2 ITIL

V kontextu standardu ITIL se nepoužívá termín Disaster Recovery[4], ale termín (či lépe název procesu) IT Service Continuity Management/ITSCM. Tento proces v IT se nicméně striktně odkazuje na business process nazývaný Business Continuity Management/BCM.

Zatímco v prvním případě jde o proces určený pro útvar IT, v druhém případě jde o proces určený pro obchodní útvary.

ITSCM je procesem, který se zabývá řešení obnovy služeb IT po katastrofických událostech tak, aby obchodní procesy firmy mohly po katastrofě buďto v plném nebo částečně omezeném rozsahu pokračovat.

Oficiální definice procesu ITSCM dle slovníčku ITIL V3 (překlad itSMF CZ – viz www.itsmf.cz) je tato:

Proces odpovídající za správu rizik, která by mohla vážně ohrozit služby IT. ITSCM zajišťuje, aby poskytovatel služeb IT mohl vždy poskytnout minimální dohodnutou úroveň služeb, přičemž omezuje rizika na akceptovatelnou úroveň a plánuje obnovu služeb IT. ITSCM by měl být navržena tak, aby podporoval Správu kontinuity businessu.

BCM pokrývá analýzu a správu rizik tak, aby organizace zajistila buďto minimální požadovanou kapacitu produkce a nebo poskytování služeb za všech okolností. Cílem BCM je redukovat možná rizika na akceptovatelnou úroveň a vyvinout a udržovat plány pro obnovu obchodních aktivit v případě, že dojde k přerušení nějakou katastrofou.

Oficiální definice procesu BCM dle slovníčku ITIL V3 je tato:

Podnikový proces zodpovědný za správu rizik, která mohou mít závažný dopad na business. BCM ochraňuje zájmy klíčových zainteresovaných stran, reputaci, značku a aktivity vytvářející hodnoty. Proces BCM zahrnuje redukci rizik na akceptovatelnou úroveň a plánování obnovy podnikových procesů, objeví-li se narušení businessu. BCM stanoví cíle, rozsah a požadavky pro Správu kontinuity služeb IT.

Jak je vidět z vysvětlení a oficiálních definic procesů, jedná se v případě ITIL o něco jako „duální dvojici“ procesů – jeden za IT a druhý za business, fakticky však se jedná spíše o uspořádání, že ITSCM je podmnožinou (sub-procesem) procesu BCM.

Vysoká dostupnost (*High Availability/HA*)

Přístup nebo návrh, který minimalizuje nebo potlačuje důsledky poruchy konfigurační položky na uživatele služby IT. Řešení s vysokou dostupností jsou navrhována pro

[4] Můžete se spíše potkat s původním termínem *Contingency Planning*.

dosažení dohodnuté úrovně dostupnosti; pro snížení počtu a dopadu incidentů využívají technik jako Odolnost proti chybám (*Fault Tolerance*), Odolnost (*Resilience*) a Rychlá obnova (*Fast Recovery*).

Pozn. autora: občas se zaměňuje termín HA a DR, popř. se implementuje DR v situacích, kdy se požaduje vysoká dostupnost v rámci procesu Availability management. Je nutné zdůraznit, že HA je o zabraňování běžných poruch a druhů provozních výpadků, zatímco DR je o schopnosti zotavit se při havárii. V některých případech se však vědomě může využít DR jako opatření pro HA (speciálně v případě online replikací dat a schopnosti okamžitého přepnutí – *Immediate Recovery*).

Availability management/AvM

Availability management nebo chcete-li Správa dostupnosti je proces ve fázi návrhu služeb (Service Design), odpovědný za definování, analýzu, plánování, měření a zlepšování všech aspektů dostupnosti služeb IT. Správa dostupnosti odpovídá za zajištění přiměřené infrastruktury IT, procesů, nástrojů, rolí atd., které odpovídají dohodnutým cílům úrovní služeb v SLA.

Pro účely tohoto článku je nutné dodat, že procesy ITSCM a AvM používají některé společné techniky – typicky např. analýzu a správu rizik, navíc opatření v oblasti DR/BC mohou příznivě působit v oblasti AvM (např. při výpadku hlavního centra lze přepnout na záložní i v případě nějaké rutinní poruchy, popř. pokud provozujeme obě centra s nějakou formou rozložení zátěže, tak i rutinní porucha nevede k výpadku díky dostupnosti záložního centra)..

Je nutné ale zdůraznit, že rozdíl mezi oběma procesy je primárně v tom, že v případě AvM se snažíme o správu dostupnosti v kontextu drobných zlepšení, reaktivních opatření při různých neplánovaných výpadcích a průběžných vylepšování dostupnosti, ale pouze v kontextu **běžných poruch**. ITSCM oproti tomu se soustředí na zajištění dostupnosti služeb, resp. obnovu služeb po rozsáhlých **haváriích** a **katastrofách**.

Capacity management/CaM

Capacity management anebo Správa kapacit je procesem ve fázi návrh služeb (Service Design) odpovídajícím za to, že kapacita služeb IT a infrastruktura IT jsou schopny dodat služby na dohodnuté úrovni, za přiměřených nákladů a včas. Správa kapacit (Capacity Management) bere v úvahu všechny zdroje potřebné pro dodávku služeb IT a připravuje plány pro požadavky businessu v krátkodobém, střednědobém a dlouhodobém horizontu.

Pro účely tohoto článku je nutné dodat, že opatření v oblasti ITSCM může někdy pozitivně přispívat ke zvýšení kapacity – např. v případě, kdy máme 2 datová centra s replikací dat a provádí se rozložení zátěže (*load balancing*) mezi oběma z nich. Jiným příkladem může být situace, kdy si organizace rámci opatření na ITSCM vybudovává záložní centrum, tak většinou nabírá určitý počet lidí pro podporu druhého centra, což se v rutinních případech navyšování kapacit existujících služeb zpravidla nečiní[5].

Business Impact Analysis/BIA

BIA je činnost Správy kontinuity businessu (Business Continuity Management), která identifikuje vitální (nezbytné) funkce businessu a jejich závislosti. Tyto závislosti mohou zahrnovat dodavatele, personál, další podnikové procesy, služby IT atd.

[5] Známá strategie vyšších managerů – „*do it more (work) with less (money)*“.

Business Impact Analysis (BIA, česky též analýza dopadů, analýza dopadů na business) tvoří jeden ze základních stavebních prvků uceleného procesu řízení kontinuity činností (zpravidla podnikatelských, resp. ekonomicky výkonných) podniku. Koncepčně vychází BIA z obecné metodologie a postupů pro řízení rizik, avšak cíleně se soustředí na identifikaci klíčových podnikatelských činností/výstupů/produktů organizace a hodnocení vlivu výpadků či narušení realizace těchto činností příp. podpůrných činností (např. procesy a služby IT, výpadky lidských zdrojů apod.) na ekonomickou výkonnost podniku, jeho reputaci, prostředí, v němž daný podnikatelský subjekt působí či společnost (ve smyslu sociálním).

BIA definuje požadavky na obnovu služeb IT . Tyto požadavky zahrnují cíle definující maximální trvání obnovy (*Recovery Time Objectives*), cíle pro obnovu k určitému bodu v čase (*Recovery Point Objectives*) a minimální cíle úrovně služby pro každou službu IT.

CRAMM

CCTA **R**isk **A**nalysis and **M**anagement **M**ethod (CRAMM). Jedná se o metodu (a také SW), který umožňuje identifikaci aktiv (*Assets*), registraci možných ohrožení (*Threats*), definici zranitelností (*Vulnerabilities*) a vyčíslení reálných rizik (*Risks*). Na základě těchto hodnot je potom možné navrhnout adekvátní protiopatření sloužící buďto ke kompletní eliminaci těchto rizik nebo aspoň snížení jejich pravděpodobnosti či snížení negativních dopadů na business firmy.

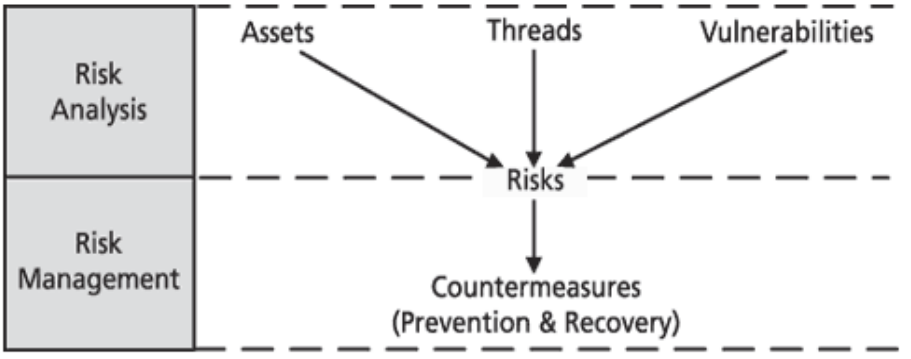


Figure 13.2 The CCTA Risk Assessment Model (source: OGC)

2. Trendy v oblasti DR/BC

Dle některých studií jako např. Forrester ([1]) firmy na korporátní úrovni převážně prohlašují, že jsou na takové případy připraveni. Ve většině případů to není tak úplně pravda a jedná se často o situace, kdy firmy prostě tvrdí něco, čím si nikdy neprošli (podle např. zmíněné studie 36 procent z nich neprodělalo žádnou katastrofu, aby mohli objektivně říci, že jsou připraveni).

Poměrně častým trendem rovněž je outsourcing DR v různých podobách – od kompletního outsourcingu až po dílčí outsourcing třeba záložních datových center apod. Většinou jde o největší firmy jako je Hewlett-Packard, IBM Corp. či SunGuard. Podle údajů firmy Forrester z května 2010 se počet firem uvažujících o outsourcingu v letech 2008-2009 zdvojnásobil na více než 44 procent a očekává se další růst.

Podobně je na tom další velmi aktuální trend dneška – Cloud Computing/CC. Gartner předpovídá pro rok 2014, že vzroste procento firem uvažující CC jako další strategii pro DR umožňující zvýšit odolnost jejich kritických aplikací až na 15 procent.

Dalším důvodem pro optimismus mohou být i technické aspekty provádění DR, kdy se od původního zálohování na pásky postupně čím dále víc přechází na replikace dat ve 2 či více datových centrech a kopie dat na další typy nosičů.

Toto je ostatně velmi zajímavý trend: zatímco se technologie a technika vyvíjí slibně ve prospěch RD/BC, ve většině případů to však ani trochu neznamená, že bychom tuto oblast měli jakkoliv ignorovat, neměli se starat o solidní strategii v této oblasti a nemít připravený akční plán. V praxi je plánování, testování a údržba těchto plánů klíčová pro udržení připravenosti.

Docela významnou součástí trendů v oblasti DR/BC je také snaha o maximálně portabilní komunikaci – instrumenty jako SmartPhones, dynamické komunikační protokoly od firem jako je IBM (Lotus), Microsoft (OCS) či Cisto zase nabízejí různé formy komunikace v případě havárií apod.

Hodně důležitou roli také hraje oblast automatického testování. Tato technika nyní velmi významně používaná ve vývoji pro funkční a výkonnostní testování se dá s úspěchem použít i v oblasti DR, i když je jasné, že úplně lidský činitel nenahradíme nikdy. Dokážeme tak poměrně dost dobře ušetřit náklady na testování DR.

Když již hovoříme o technologických trendech, bylo by špatně nezmínit virtualizaci. Některé SW výrobci těchto nástrojů nabízí možnost automatizace přechodu na DR do záložních lokalit – příkladem může být např. VMWare se svým nástrojem Site Recovery Manager. Jiní výrobci zase nabízejí možnosti konverze fyzických serverů na virtuální v případě katastrofy. VMWare, Citrus a někteří další nabízejí i možnost tzv. virtualizace desktopů umožňující vzdálené připojení – např. pro případy globální pandemie chřipky apod. Virtualizace také poměrně dobře umožňuje provádění automatizace některých rutinních operací v oblasti DR a tím šetřit náklady.

3. Nejčastější chyby v oblasti DR/BC pro IT

V následujícím textu jsou postupně rozváděny nejčastější problémy a chyby, se kterými jsem se ve své praxi potkal. Některé z nich jsou spíše namířeny vůči DR, jiné zase vůči BC, ale většinou platí obecně. Uvědomme si v této souvislosti, že např. informace o zákaznících (zákaznický informační systém) patří jak pod DR, tak ale i pod BC, neboť toto je základní vitální informace pro zachování businessu.

3.1 Seniorní management bere DR/BC na lehkou váhu

Potkal jsem se osobně s tímto fenoménem hodně krát. Nejvyšší manageři musí být z principu své funkce velmi optimističtí a přicházet pokud možno hlavně s pozitivními scénáři vývoje společnosti (to v praxi znamená růst). Souvisí to se známými úvahami známých profesorů na *Harvard Business School*, kteří se velmi seriózně zamýšlí nad tím, jestli extrémní starost o rizika a hlavně regulativní standardy a zákony nebrání ve finále firmám ve zdravém podnikání.

Postupem, který ve většině případů nikam nevede, je pokus vaše managery vystrašit, to zpravidla nefunguje a hlavně nositelé těchto zpráv je pak někdy označován za škarohlídy a nikdo z businessu se jich pak už zpravidla neptá ani na názor apod.

Daleko účinnější metodou je zdůraznění, že BC je součást celkové *Corporate Governance* a snahou minimalizovat provozní výpadky a udržet firmu v chodu zaváděním opatření zvyšujícím celkovou odolnost proti chybám, vyšší dostupnost služeb či vyšší kapacitu a nikoliv pouze poskytnout ochranu proti haváriím[6]. Při vysvětlování je nutné klást důraz na možný negativní dopad na organizaci v případě takovýchto výpadků, bez ohledu na to, čím byly způsobeny, a efekt, jaký to může mít na každodenní plnění cílů firmy, včetně snížení reputace a finančních výsledků. Zkuste naopak zdůraznit pozitivní vlivy těchto opatření a politik jako nástroje marketingu, demonstrující vaši lepší připravenost než vaši konkurenti a schopnost obstát před vašimi akcionáři.

Výše doporučený postup do jisté míry zvolil např. britský Vodafone, když se po zralé úvaze rozhodl pro certifikace oproti normě BS 25999 a formulovat to jako strategii, jak se zviditelnit proti konkurenci.

Velmi užitečným cvičením je v této situaci uspořádání nějakého dvouhodinového workshopu pro váš seniorní management ilustrující jak se vaše firma bude chovat v případě nějaké rozsáhlé havárie a to jak na úrovni IT, tak i businessu. Tento postup zpravidla zvyšuje informovanost, odhalí úzká místa ve vaší argumentaci, případně vašich plánech a motivuje všechny se o tom znovu sejít a pravidelně se o tom bavit.

3.2 DR není jen záležitost IT, či jinak řešeno DR není BCM

Velmi často se mlčky předpokládá, že obě věci znamenají totéž, to ale není pravda ani zdaleka. To ostatně již vyplývá z jejich definic uvedených v preambuli tohoto článku.

Obnova výpočetní techniky a dat je pouze mandatorní stránka věci, ale stejnou, ale spíše větší úlohu hrají uživatelé a business.

BCM by se rozhodně neměla řešit v serverovně, ale v obchodních útvarech. IT pak teprve následně může řešit adekvátní uspořádání pro DR.

IT sice v celé řadě případů formálně deklaruje, že rozumí požadavkům businessu (říká, že někdy lépe než lidé z businessu), ale při detailním pohledu zjistíme, že to není pravda. Zatímco to může být pravda v ojedinělých případech, kdy se koncoví uživatelé, speciálně ti starších ročníků, trochu „perou“ s výpočetní technikou a způsobují minimálně zvýšené obočí personálu IT; v případě podnikových procesů a jejich detailní znalosti je tomu zpravidla kompletně obráceně – pracovníci IT nemají „páru“, jaké jsou třeba priority businessu, co daná služba z pohledu businessu obnáší či v jakém pořadí obnovovat služby v případě havárie.

Jednu věc je zde nutné zdůraznit: implementace chybných, neadekvátních, nedotažených nebo nekompletních řešení je vyhazování peněz oknem. Plány pro BCM a DR by zásadně měly vycházet z provedené analýzy dopadu BIA, z požadavků businessu na obnovu a korektní kalkulace rizik.

[6] Podle některých studií stojí za snahou implementovat DR/BC z cca 70 procent snaha zajistit vyšší dostupnost služeb, z 25 snaha zabránit neplánovaným výpadkům a pouze ze zbývajících 5 procent snaha ochránit firmu vůči přírodním katastrofám.

3.3 Chybějící nebo chybné zálohování dat

Zálohování dat se provádí nekorektním způsobem, nepravidelně, popř. vůbec. Tento bod se v praxi může rozpadat do celé řady dalších bodů:

- Ignorování některých best practise v oblasti zálohování – např. zásada více kopií, bezděčné přepisování apod.
- neprovádí se testování záloh dat
- nedůsledná nebo chybějící evidence záznamů o zálohování a archivaci
- šetří se na záznamových médiích a ty se používají ve větší intenzitě, než kterou garantují jejich výrobci – výsledkem je potom nemožnost načíst data ze zálohy díky poškození magnetické vrstvy
- provádění zálohování formou delty se ztrátou primárních dat
- ukládání záloh ve stejné a nebo blízké lokalitě
- ignorování varovných hlášek v logu při zálohování atd.

Je pravdou, že zálohování je skutečně nudná záležitost a ve většině případů zbytečná. Do té doby, než data ze zálohy skutečně potřebujete.

Můj kolega, specialista na databáze a SAP mi vyprávěl příhodu, která se mu přihodila u známé firmy v oblasti utilit. Tato firma provozovala systém SAP, včetně řízení výroby. Systém byl sice zálohován na úrovni databáze, ale nikdy se neprovádělo otestování této zálohy. Výsledkem potom bylo, že záloha po nějaké provedené změně v průběhu let neobsahovala kompletní zálohu všech datových souborů, ale jeden z nich chyběl. Jednoho dne došlo k neopravitelné poruše jednoho z diskových polí tak, že již nebylo možné obnovit data prostým zrcadlením disků. Bylo proto nutné použít zálohu dat. Přitom se zjistil výše uvedený problém a databázi již nebylo možné nijak obnovit. Celá příhoda měla samozřejmě konsekvence nejen v zastavení výroby, ale i ve výpovědích pro odpovědné pracovníky a ve finále vyústila v situaci, kdy výkonný ředitel firmy žádal dopisem všechny zákazníky a partnery, aby mu poskytli kopie faktur za poslední 2 roky.

Další věcí může být fakt, že vy můžete být špatně připraveni na DR, obnova vám může trvat daleko déle, než jste si kdy byli ochotni připustit, ale bez zachování a obnovy dat pomocí zálohování (popř. replikace) dat nemusíte být schopni provést obnovu **nikdy**.

3.4 IT si musí zjistit, jaké služby (aplikace) jsou nejvíce prioritní a jaké je pořadí obnovy

Zatímco IT hodně často slyší, že služby (či lépe řečeno business procesy) typu CRM, billing, ERP, ECM jsou missiona critical, ale velmi často neví, co to vlastně znamená, jaké služby IT to v praxi obnáší.

V některých případech existují velmi silné závislosti na dodavatelích třetích stran, či závislosti na dalších službách, které bezprostředně nebyly zmiňovány jako mission critical.

2 příklady za všechny:

Velký telekomunikační operátor v ČR provozoval systém SAP jako 24x7 mission critical službu, ale nikoliv již některé podpůrné infrastrukturní služba jako je např. DNS či NFS (ta první infrastrukturní služba zajišťuje tzv. zpětný překlad symbolických jmen na IP adresu, ta druhá může např. sloužit k ukládání příloh). Výpadek té první služby pak mohl způsobovat nemožnost přihlášení uživatelů do SAP, zatímco výpadek druhé služby zase nemožnost přístupu k přílohám, které mohou obsahovat velmi důležité informace. Na této úrovni detailu definic služeb a jejich závislostí může pracovat pouze IT, business většinou nemá reálnou představu, z čeho se ve skutečnosti balík služeb SAP skládá. Tento rozpor zde odhalilo až nasazení CRAMM.

Celá řada velkých firem se zaklíná, že mají provedenu analýzu BIA[7] za pomoci významných a renomovaných poradenských firem. Podobně i jedna z největších bank v ČR. V momentě kdy HP před lety jako dodavatel nikoliv BCM, ale ITSCM začal společně s pracovníky provozu budovat celé řešení, přišla v potaz samozřejmě tato analýza BIA. Při bližší analýze se zjistilo, že je zde poměrně hodně dobře provedena základní prioritizace služeb, kompetentní analýza potenciálních ztrát při výpadku těchto služeb, ale již nebyla nikterak řešena situace, kdy např. v případě výpadku celého primárního datového centra dojde k několikanásobnému výpadku těchto služeb a je třeba rozlousknout, kterou z těchto služeb je nutné obnovit jako první. Ve zmíněném případu došlo k neshodě na úrovni jednotlivých divizních ředitelů a ve výsledku finální pořadí obnovy musel určit CEO.

3.5 Nejsme připraveni na všechno

Někdy se říká, že po bitvě je každý generál a platí to i pro oblast BC/DR. Zde to někdy fakticky vypadá, že utratíme spoustu peněz za opatření, které mají řešit aktuální katastrofy – v Evropě třeba povodně a ve Spojených státech třeba hurikány. Jakkoliv chápeme tuto strategii jako sebeobrannou, havárie a katastrofy jsou v principu nepredikovatelné.

Pokud zůstaneme u známých příkladů, vezměme si například situaci ze Spojených států - 11. září 2001, kdy atak teroristů devastoval celou řadu firem v oblasti finančních služeb. Mnohé z těchto firem totiž měli záložní zařízení v druhé budově z tzv. „dvojčat“. Po této události se firmy poučily a pustili se za ohromné peníze do výstavby záložních datových center kolem řeky v oblasti Jersey. Bohužel další katastrofa v oblasti Manhattanu, která se zde stala v r.2003, byl kompletní výpadek elektrické energie (*blackout*), který zasáhl i celou oblast Jersey. Ve výsledku se tedy všechna provedená opatření ukázala v praxi jako zbytečná, protože došlo k výpadku i záložních center.

Jediným způsobem, jak toto řešit, je provést detailní analýzu rizik, jasně klasifikovat vaše největší aktiva, identifikovat možná rizika a pokusit se odhadnout jejich pravděpodobnost.

3.6 Provádění fiktivních testů, podvádění, podcenění

Je jasné, že DR je hodně spojováno s testováním. To je však hodně náročné na zdroje a čas, výsledkem je potom snaha o automatizaci testů, zjednodušování procedur pro přechod do záložního stanoviště, což je rozumné a nebo naopak ignorance ze strany businessu, snaha o obcházení či omezené provádění testů, což je rozumné už daleko méně. Přičteme-li k tomu navíc přirozenou snahu pracovníků se cíleně vyhýbat tak

[7] Business Impact Analysis.

nezáživné činnosti, jakým bezesporu testování je, nemůžeme se divit, že se někdy i podvádí.

Chci v téhle souvislosti odkázat na ITIL „best practise“. Při nedávném školení na ITIL PPO certifikaci se objevila otázka, zda by se měl v rámci opatření v procesu ISCM provádět plný test (*full test*) či jenom částečný (*partial testing*) či jen test na sucho (*dry test*) a zda by se případně měl pravidelně opakovat. Zatímco ITIL v celé řadě případů zaujímá poměrně uvolněné stanovisko připouštějící různé interpretace, je v této oblasti totálně striktní – test by se měl provádět opakovaně a formou plného testu a to za všech okolností.

3.7 Plán na DR není specifický, DR plán se nedá zkopírovat

Implementace SW pro DR nebo „vysokozdvižné“ scénáře na téma „co, uděláme když?“ ani zkopírování scénářů z internetu či od „konkurence“ nestačí. Je nutné si v prvé řadě uvědomit, že plány na BC vždy a na DR ve většině případů jsou specifické podle potřeb firmy. Dále je nutné zajistit, aby DR tým byl dobře zběhlý v plánu na DR a tento plán byl pečlivě otestován a ověřen. Personál IT, stejně jako vyšší management by měl být detailně vyškolen v provádění procedur DR v případě jakékoliv katastrofy. Rozhodně se v době aktivace DR/BC jedná o krizové řízení a není možné nic ponechávat nic na rozhodování typu ad-hoc.

Další potenciální alternativou tohoto bodu může být situace, kdy např. organizace přebírá plán od jiné organizace (např. outsourcer od zákaznické firmy), případně dceřiná společnost (potenciálně vybavená jinou infrastrukturou, jinak organizovaná a poskytující jiné služby) od mateřské firmy. Zde je asi v pořádku přebírat generické koncepty a inspiraci od někoho jiného, ale plán by měl být určitě specifický pro danou firmu zohledňující její business procesy.

3.8 DR není jen věcí IT

Katastrofy ovlivňují celý business, nejenom infrastrukturu IT. Reprezentanti ze všech oddělení firmy by se měli zúčastnit nejenom plánování, ale měli by také znát svou roli v případě katastrofy. Navíc je nutné vyškolit exekutivní management firmy a pracovníky provádějící rozhodnutí v provádění plánu DR. Měli by být znalí všech procedur a být zahrnuti v testování.

3.9 Pořizování levného, nekvalitního HW

Je doba šetření ve všech oblastech. Všichni pracovníci IT dnes jsou nuceni pracovat s omezenými rozpočty a tak mají tendenci kupovat HW za nízké ceny. Jiným poměrně častým zlozvykem se také stalo, že se zařízení do záložního datového centra kupuje buďto neznačkový a nebo ne úplně ekvivalentní HW z hlediska sizingu. Výsledkem je potom zařízení s vyšší chybovostí či ne úplná náhrada primárního centra.

3.10 Nejasné pravomoci, aneb kdo velí?

Zatímco v některých oblastech jako je např. zdravotnická péče, armáda a policie, máme jasně definovány způsoby „velitelského“ řízení, u BR/DR tato problematika zpravidla bývá podceněna. Do některých pozic je nutné vybrat pečlivě rozumné jedince – managery mající zpravidla schopnost uvážlivého, ale rychlého rozhodování – krizový manager.

Nedílnou součástí tohoto cvičení je určení klíčových procesních rolí a nominování příslušných jedinců, včetně vyřešení jejich zástupnosti. A zde nejde jenom o dovolené či nemoci zaměstnanců, ale je také nutné si uvědomit ,že v situacích havárií a katastrof může také dojít (a v praxi dochází) ke zraněním či smrti některých zaměstnanců, takže plány a procedury na DR/BC musí být psány takovým způsobem, aby je bylo možné použít i neexpertním pracovníkem.

3.11 Příliš obecná dokumentace

Klasickým problémem bývá úroveň dokumentace. Jak již bylo uvedeno v předcházejícím bodu, pro DR/BC potřebujeme poměrně podrobnou úroveň dokumentace, podle které budeme postupovat i v případě, že nám chybí klíčoví pracovníci.

3.12 Není definován tým pro krizové řízení BCM/DR

Dosti často se stává, že existuje plán BCM i DR, ale nejsou určeni příslušní pracovníci do definovaných rolí. Výsledkem je, že v době katastrofy je obnova nefunkční a selhává na neurčených jedincích.

3.13 Podcenění významu informovanosti zaměstnanců

Ve standardech ITIL a CobIT se potkáte s termíny „*awareness*“ či „*communication plan*“. Oba výrazy mají jedno společné – zdůraznit nutnost informovat zaměstnance. U DR/BC to musí platit dvojnásob, uvědomme si, že jde o situace, kdy hrozí ztráty nejenom na majetku, ale i životech a zdraví zaměstnanců. Neinformovaný zaměstnanec pak může zhatit i dobře míněné plány na DR/BC.

Postupy při DR/BC by měli být uloženy na několika místech a to nejenom v elektronické podobě, aby se zajistilo, že budou k dispozici i v případě havárie. Důležitou informací je i informace o záložním datovém centru, stejně jako zajištění způsobu dopravy, jaký se předpokládá se sem dostat.

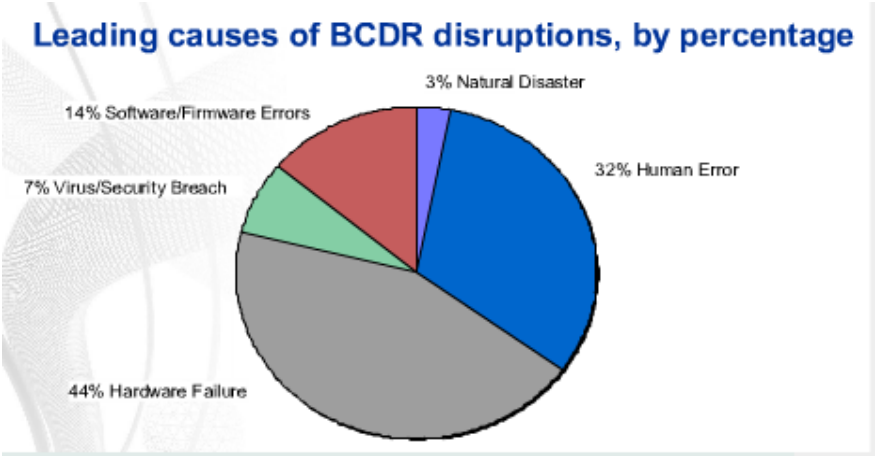
Obecně zde platí, že zaměstnanci by měli být nejenom pravidelně informováni o těchto plánech, ale také proškoleni a to specielně ti, kteří hrají v plánech pro DR/BC hlavní roli. Ideální je, pokud je do vytvoření a následného plánování, testování a aktualizace těchto plánů zainteresováno co nejvíce zaměstnanců. Tím se zajistí ta nejlepší informovanost bez nějakých extrémních nákladů na implementaci.

4. Osobní doporučení na opatření v oblasti DR/BC

Asi by se dalo očekávat, že zde prostě shrnu všechny v předchozí kapitole probírané neduhy a prostě u nich otočím znaménko. Ne až tak úplně, v některých případech je potřebné ještě některé věci specificky doplnit.

4.1 Ujasněte si procentuální příčiny havárií

Jedna z hodně podceňovaných věcí je rozpoznání, co je nejčastější příčinou těchto událostí. Jakkoliv je obecné mínění založeno na předpokladu, že to jsou primárně živelné události jako jsou povodně, požáry, tornáda či tsunami a zemětřesení, je možná překvapivé, že přírodní pohromy tvoří pouze 3 procenta všech událostí – detaily – viz následující obrázek.



Jak vidíme, hlavní příčinou číslo 1 je porucha HW následovaná hned v úzkém závěsu číslem 2 – lidskou chybou. Proto je vhodné a já to vysoce doporučuji nasazení některých formálních metod ERM či alespoň CRAMM v oblasti DR. Tyto metody berou totiž v potaz pravděpodobnosti jednotlivých ohrožení a umožňují tak rozumnou prioritizaci opatření na DR/BC.

4.2 Ujasněte si reálné potřeby businessu v případě mimořádné události

V celé řadě případů se vám může stát, že zjistíte, že reálné potřeby businessu nevyžadují nějaké extrémní opatření – např. v situaci, kdy jste buďto v monopolním nebo majoritním postavení. Pokud jde o situaci, kdy jste korektně provedli BIA i analýzu rizik a výsledkem je „oblíbené“ řešení (*recovery option*) BCM/DR u některých našich firem – „*Do Nothing*“. Pokud je toto vaše navrhované opatření po provedení pečlivé a korektní analýzy rizik a zvážení dopadů výpadku takové služby na business, pak je vše v pořádku.

Kombinujte opatření v oblasti BCM a DR, neprovádějte je odděleně.

4.3 Ani pokud vaše firma neprovádí BCM, buďte v IT připraveni provádět DR

Protože se často potkávám se situací, kdy něco jako BCM plány ve firmě vůbec neexistují, nabízí se logické řešení pro IT tuto problematiku rovněž ignorovat. Pokud mohu jen trochu radit, jděte raději příkladem a mějte definována alespoň základní opatření, co budete dělat v případě havárie.

Docela dobrým způsobem, jak takovou věc komunikovat s businessem jsou SLA, resp. definice katalogu služeb. Pokud se pouštíte do této oblasti, „nestyďte“ se před businessem argumentovat, že nemáte DR pro dané služby. Pokud se nad tím podiví, argumentuje odkazem na shoření tovární haly, vyplavení budovy nejvyššího managementu a ptejte se, jak jsou oni na tyto situace připraveni. Moje zkušenost je, že se zpravidla potom dojde alespoň k rámcovým dohodám. Určitě mějte provedenu BIA alespoň v omezeném kontextu na úrovni služeb IT.

4.4 Kromě BIA proveďte také regulérní analýzu rizik

Je fajn, že má vaše firma korektně zpracovánu analýzu BIA, je ale nutné toto ještě doplnit celým ansámblem opatření v oblasti ERM. Některé poradenské firmy jako třeba Forrester či Gartner dokonce doporučují obě disciplíny vést jednotně pod jedním vedením. To se však nevyskytuje příliš často, většinou jsou tyto oblasti vedeny odděleně, což je poměrně logické, ERM má většinou daleko širší rozměr než BIA.

Každopádně BIA vám pomůže odhalit negativní dopady na business v případě výpadku klíčových služeb, ale pečlivá analýza v rámci ERM vám pomůže odhalit, jaká skutečná rizika vám mohou hrozit a hlavně umožnit nadefinovat konkrétní protiopatření proti jednotlivým hrozbám a nikoliv jen činit obecná opatření.

4.5 Udržujte plány pro DR/BCM aktuální

Mnoho managerů si myslí, že implementace těchto procesů (ať už podle ITIL a nebo mezinárodních norem, případně i podle lokálních regulativních standardů) je jednorázová záležitost, ale to není pravda. Pokud neudržujete plány aktuální, rovná se to v podstatě pouze zbytečnému vyhazování peněz.

Udržujte plány pro BC a DR aktuální, ideálně ve vazbě na procesy Configuration managementu/CfM a Change Managementu/ChM – tedy jakákoliv změna např. v číslovacím plánu IP adres v primárním datovém centru musí být v rámci ChM promítnuta do aktualizace dokumentace a provedení adekvátních změn také v sekundárním datovém centru apod.

4.6 Určete odpovědnosti až na úroveň jednotlivých osob

Zásadně by mělo platit, že máte určeny a obsazeny všechny klíčové pozice v rámci plánů pro BCM a DR, abyste mohli uplatnit krizové řízení. V praxi to znamená reprezentanty z provozu, IT, financí, právního oddělení, HR, PR, správy budov a bezpečnosti. K tomu přidejte seniorního managera jako krizového managera. Pro každou roli by samozřejmě měl existovat zástupce, oficiálně jmenovaný.

Implementujte jasný eskalační proces, ujasněte si kontakty pro mimořádné události a proveďte školení všech zaměstnanců. Tak zajistíte, že v případě události (ať už aktuální nebo potenciální) je aspoň 1 člen krizového týmu uvědoměn a může odhadnout, zda je potřeba jednat či nikoliv.

Připravte se na situaci, že se havárie stane v době, kdy budou vaši zaměstnanci v práci, to znamená organizovat pravidelně evakuace a aspoň jednou cvičný přesun do záložního centra. Během těchto akcí se zjistí, co je nutné zlepšit a jak jsou vaši zaměstnanci připraveni na krizové situace.

Nezapomeňte také na zdánlivé samozřejmosti, jak uspět: mít za všech okolností zajištěna zálohovaná data a dostupné plány pro BCM/DR uložené mimo vaši firmu. Důležitou roli hraje v tomto kontextu také role vašich dodavatelů, mějte pod kontrolou jednak komunikační plány a hlavně smluvní ujednání o plnění v případě nějaké katastrofy.

4.7 Předpokládejte spíše to nejhorší, nikoliv to nejlepší

Dosti častou chybou je spoléhání v oblasti BC/DR na „junácké štěstí“ či na fakt, že se žádná taková katastrofa mé firmě ještě nestala. To je ovšem velmi nebezpečný postup,

specielně v kontextu zvyšujících se přírodních katastrof, nebezpečí terorismu či špionáže, a hlavně všude objímající globalizace a zvyšující se konkurence.

Zkušenosti ukazují, že mnohdy se jde o na velmi řídce vyskytující se katastrofy poměrně dobře připravit.

4.8 Testování

Proveďte aspoň jednou plný test vašeho DR a pak průběžně testujte pouze dílčí úlohy, např. jenom určité služby, popř. se zaměřte na prověření určité skupiny/útvaru IT. Maximalizujte v maximální možné míře automatizaci takových testů, jak je to jen možné. V počátcích využívejte testování „na sucho“ formou pročítání dokumentace s kontrolou znalostí a za účasti externích auditorů či konzultantů, kteří vám mohou poradit a objektivně posoudit míru testování. Nezapomeňte, že nedílnou součástí testování je také odstraňování nedostatků, resp. zajištění průběžných změn a zlepšování. V neposlední řadě berte v potaz, že úspěšný test by měl být vždy prováděn za účasti pracovníků z businessu. V případě, že dojde k významné změně potřeb businessu, podnikových procesů či významné změně infrastruktury, počítejte s tím že je nutné zopakovat plný test DR/BC znovu.

5. Závěr

Tento článek se snažil ilustrovat nejčastější chyby prováděné v oblasti DR/BC a zároveň navrhnout způsob, jak se jim předcházet a jak je řešit. V celé řadě případů se jedná o opatření, která nemusí nutně přinášet nějaké obrovské náklady a úsilí, neboť nesměrují jen do oblastí technologií a pořizování HW a SW, ale hlavně do oblasti řízené lidských zdrojů a vychovávání a školení pracovníků, jak na straně IT, tak i na straně podnikových útvarů. Ale určitě platí, že investice do této oblasti jsou pořád jedny z nejvyšších, proto je nutné velmi pečlivě zvažovat jednotlivé varianty opatření na DR a jejich dopad na business.

6. Literatura:

[1] http://www.casact.org/research/erm/overview.pdf

[2] http://www.coso.org/

[3] http://www.aicpa.org/Pages/Default.aspx

[4] http://www.nfpa.org/assets/files/PDF/CodesStandards/TIAErrataFI/ProposedTIA948NFPA1600.pdf