COMMERZBANK

Návratnost investic do informační bezpečnosti

itSMF

Hotel Diplomat, Praha

10. 11. 20010

Ing. Zdeněk Blažek, CSc. CISM
zdenek.blazek@commerzbank.com
GSM: 603200858

COMMERZBANK

Návratnost investic do informační bezpečnosti

› Agenda

- Jaké jsou hodnoty, které chráníme?
- Hodnota lidské práce v IT-jak určit
- Úroveň bezpečnosti – lze měřit?
- Určení návratnosti vynaložených prostředků – přístupy
  - Rizika
  - Výpočtem

Hodnota dat/informace - materialita

- **Informace je materialitou tehdy, jestliže její opomenutí, ztráta nebo změna mají vliv na ekonomické rozhodování uživatelů, které je založeno právě na finančních úvahách. Materialita závisí jednak na velikosti položky nebo na vyhodnocení problémů, které může opomenutí, ztráta nebo změna způsobit.**
- **<u>Materialita tak poskytuje prahovou hodnotu.</u>**

COMMERZBANK

Náklady na lidskou práci v IT

Počet zaměstnanců	N
Počet IT zaměstnanců	Nit
Plocha firmy	S
Plocha využitá IT	Sit
Cena za nájem/odpisy/rok	P
Cena/m2 placená IT/rok	Pr
Cena za vodu/zam./rok	H
Cena za el./zam./rok	E
Prům. náklady na školení IT/zam./rok	T
Cena za plyn/zam./rok	G
Cena ostrahy/zam./rok (zahrnuje i náklady na EZS ...)	Sec
Prům. mzdové náklady/IT zam./rok	W
Odpisy IT prostředků/zam./rok	O
Cena podpory IT ext./zam./rok	X

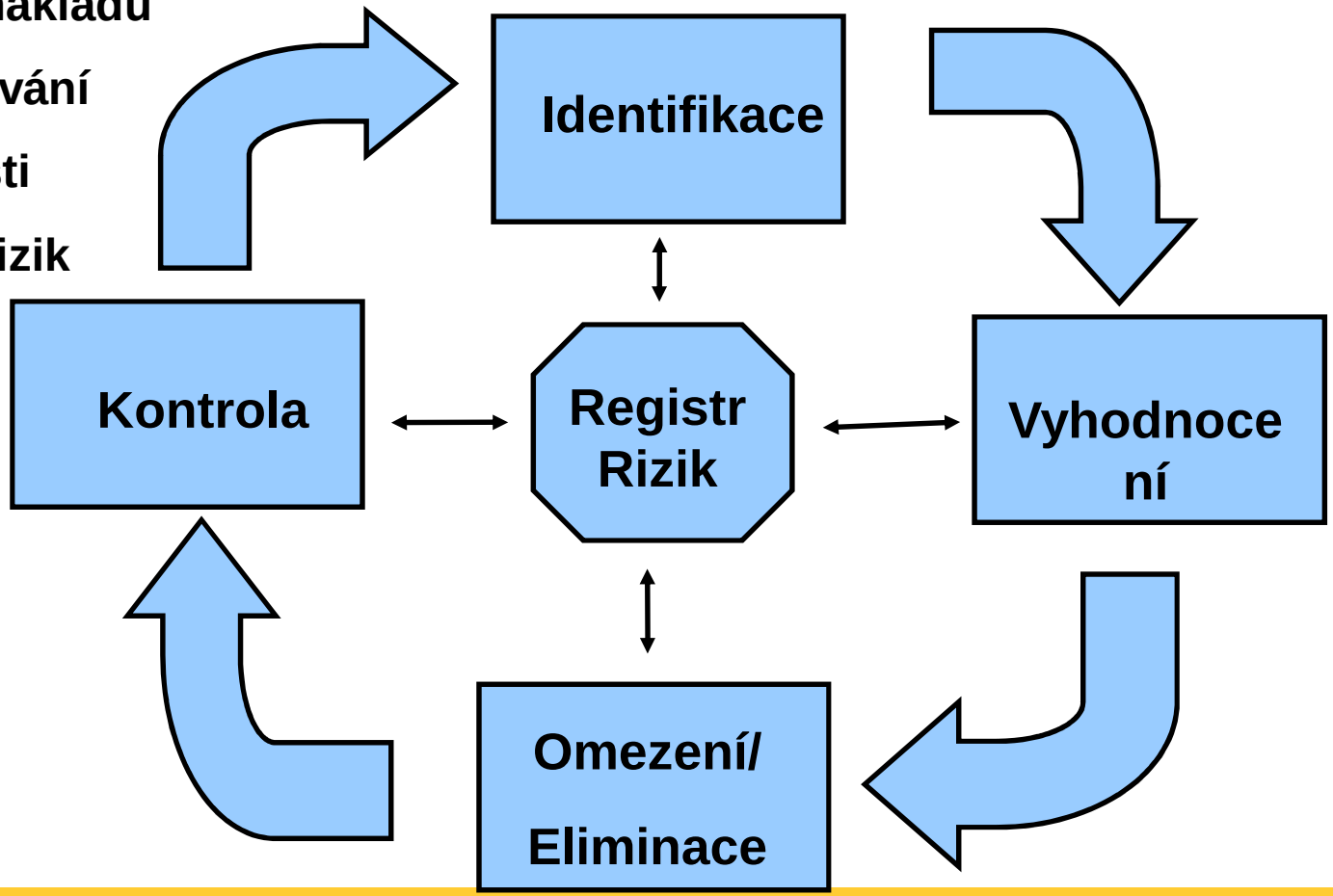
(H + E + G + Sec + W + T + O + X + (P*Sit/S*Nit))/365 = prům. cena IT člověkodne

Měření informační bezpečnosti

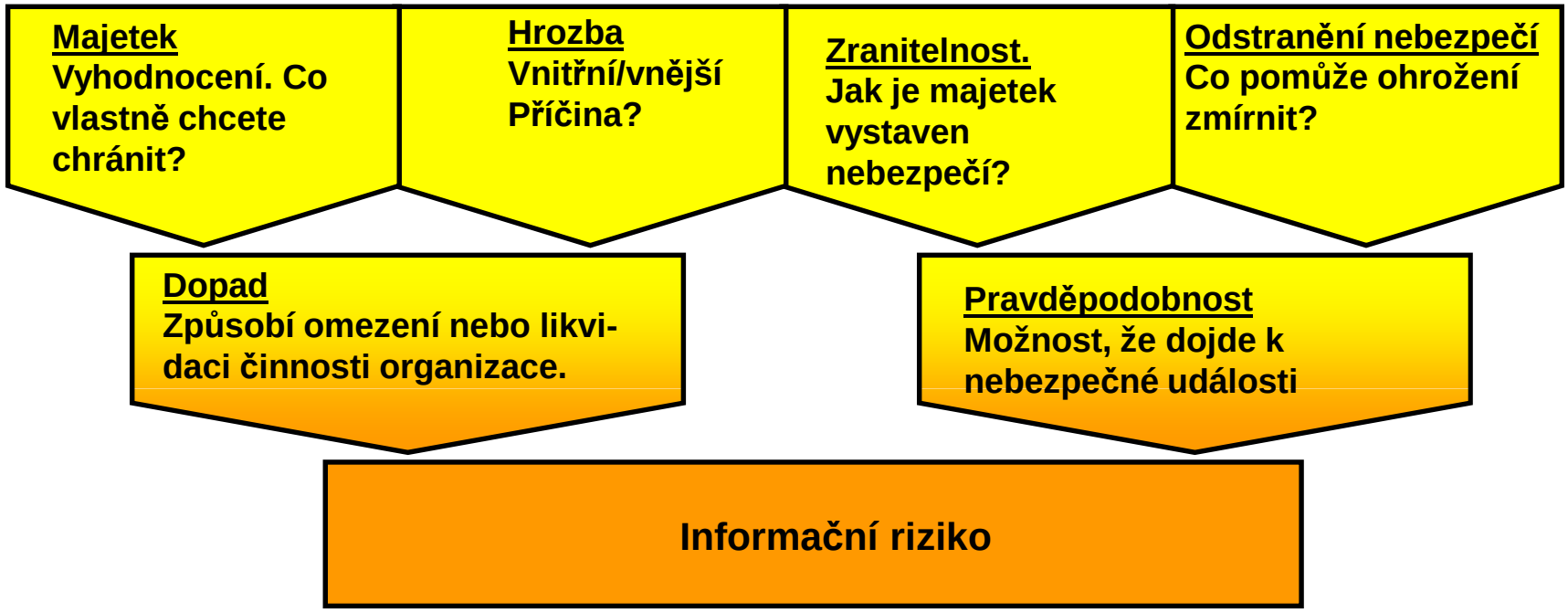
1. Co máme na mysli pod pojmem bezpečnost?
2. 100% bezpečnost neexistuje
3. Zásadní rozdíl mezi bezpečností a zabezpečením
4. Lze stanovit úroveň zabezpečení - ne bezpečnosti
5. Co vlastně chceme chránit – klíčová otázka
6. Jak to chceme chránit?
7. *Stojí to co chceme chránit za vynaložené prostředky?*

Postupy při sledování ROISI

- - Sledování informačních aktiv
- - Sledování nákladů
- - Vyhodnocování zranitelnosti
- - Sledování rizik



Řízení informačního rizika



Informační riziko definujeme jako pravděpodobnost, že dojde k narušení činnosti organizace – dopad události

Informační riziko = dopad x pravděpodobnost

COMMERZBANK

Kategorie hrozeb

Kategorie	Popis
chybná funkce	**funkční chyba technického zařízení, systému, ...**
lidská chyba	**chyba zanesená lidským faktorem-chybné zápisy,. překliknutí...**
nepředvídané dopady změn	**neočekávaný problém zaviněný nesprávným řízením změn**
přerušení dodávky služeb	**Přerušení dodávky služeb společností – různé příčiny (epidemie, živly, politika)**
vnější útok	**útok z vnějšího prostředí-fyzický/digitální. Pod tuto kategorii řadíme i útoky způsobené např. epidemií...**
vnitřní chyba použití	**nesprávné použití dat, prostředků apod.**
krádež	**Data nebo zařízení jsou ukradena (může být vnitřní/vnější)**

Vyhodnocení - metody

Metody vyhodnocení rizika jsou:

- **Kvalitativní**
- **Kvantitativní**
- **Hybridní**

Zodpovědný výbor/jedinec pak může vyhodnoti situaci a připravit

- **Doporučení pro vedení organizace/projekt – nutnost demonstrovat ROISI**

Vedení organizace pak rozhodne o:

- **Odstranění rizika**
- **Přenosu rizika**
- **Přijetí rizika**
- **Vyvarování se rizika**

Výpočet návratnosti investic do IB

1. **Obranné mechanismy proti vnějšímu útoku jsou samozřejmostí**
2. **Obrana proti vnitřnímu útoku podceňována-pravděpodobnější**
3. **IT oddělení implicitně odstraňuje zranitelnosti systému:**

a. **„F“** definujeme jako roční náklady k odstranění zranitelností systému (licence apod.)

b. **„B“** definujeme jako vstupní jednorázovou investici pro implementaci obranných mechanismů

c. **„M“** definujeme jako roční náklady na údržbu

- Pak dostáváme roční náklady na údržbu IB pro první rok jako:
- **Es = F + B + M**
- V následujících letech lze vyjádřit jako:
- **Es = F + M**

Výpočet návratnosti investic do IB

- Ztráta příjmů

  - Ve chvíli poškození (CIA) IB je vysoká pravděpodobnost okamžité ztráty příjmů. V zásadě jsou zde dvě komponenty ztrát:

a) Ztráta jako funkce času (t), po který byl systém neschopný provozu

b) Částka ztracená okamžitě Li (Loss immediatelly)

  - Celková ztráta pak je vyjádřena jako:

    - **Lt = Li + I * t/365**,

- kde **„I“** reprezentuje hodnotu podílu IT majetku, dotčeného incidentem

Výpočet návratnosti investic do IB

- Obecněji lze vyjádřit:

Lt = Li + A(t),

- kde A(t) vyjadřuje ztrátu dostupnosti

- V návaznosti na incident je nutno vynaložit čas, který IT personál ztratí při opravě/obnově, což reprezentuje opět náklady. Tyto náklady označme jako R. R je opět funkce času a tak dostáváme:

- **Lt = Li + A(t) + R(t)**

- R(t) reprezentuje roční náklady spojené s opravou/obnovou napadených systémů

Nutno znát cenu člověkodne/hodiny!!!!

- **Pozor na SLA-nepřímá úměra k času.**

Výpočet návratnosti investic do IB

- **Cílem jakéhokoliv programu řízení informačních rizik a tedy i bezpečnosti, je chránit informační aktiva co možná nejefektivněji, tedy také musíme mít na zřeteli, že bezpečnostní mechanismy nesmějí do systémů zavádět body *nestability* a způsobovat jeho nedostupnost. Zároveň je třeba respektovat zásadu, že náklady na zabezpečení nesmí přesáhnout hranici, která je dána velikostí a finanční situací firmy. Je tedy nastolena otázka životaschopnosti (oprávněnosti) investic do IT.**

Výpočet návratnosti investic do IB

- Životaschopnost/oprávněnost investic do IB
  - Investice i bezpečnostní projekt jsou oprávněné tehdy jestliže platí:
    - **Es < Lt**
- Nebo jinak
  - **(F + B + M) < Li + A(t) + R(t)**
  - Dle praxe se ukazuje, že organizace by měla utratit za IB podstatně méně, než jsou očekávané ztráty – ne více než jednu třetinu

Výpočet návratnosti investic do IB

- Náklady na proniknutí
- Až doposud jsme se zabývali zranitelnostmi systému bez uvažování možnosti útoku. Zranitelnost není hrozba, tedy systém, kde nejsou hrozby je bezpečný. Nutný katalog hrozeb!
- První hrozbou je bezpečnostní systém sám!

Výpočet návratnosti investic do IB

- Útok může vést k využití zranitelností ve vlastním obranném mechanismu.
- Zavedena proměnná: „CTB“ (Cost To Break), jejíž roční hodnotu lze určit takto:

CTB = Cd + Cv, kde

- „Cd“ jsou roční náklady na proniknutí do obranného systému a
- „Cv“ jsou roční náklady na využití jeho zranitelností.
- Tyto hodnoty se obecně velmi těžko určují. **Doporučení:** buď zaměstnat člověka, který se bude pokoušet systém kompromitovat a na základě jeho činnosti tyto veličiny odhadnout, nebo najmout externí firmu nebo vycházet ze statistik a přehledů.

Výpočet návratnosti investic do IB

- Poškození obranného systému

  - Poškození samo o sobě nemusí vést ke ztrátě informací, ale v každém případě musí být opraveno. Náklady na toto jsou určeny takto:

    - **D = Dd + Di**

  - Kde „Dd“ představuje náklady spojené s poškozením obranného mechanismu a „Di“ představuje náklady spojené s poškozením IT infrastruktury. Opět nemusí jít o ztrátu informací. Jde v podstatě o pravděpodobnostní funkce.

  - Takže IT bezpečnostní projekt je životaschopný tehdy, jestliže:

    - **(F + B + M) < (Li + A(t) +R(t) + D)**

Výpočet návratnosti investic do IB

- Úspěšnost útoku

- Platí, že náklady spojené s úspěšným útokem by měly být vyšší, než je cena obranných mechanismů. Tedy by mělo platit

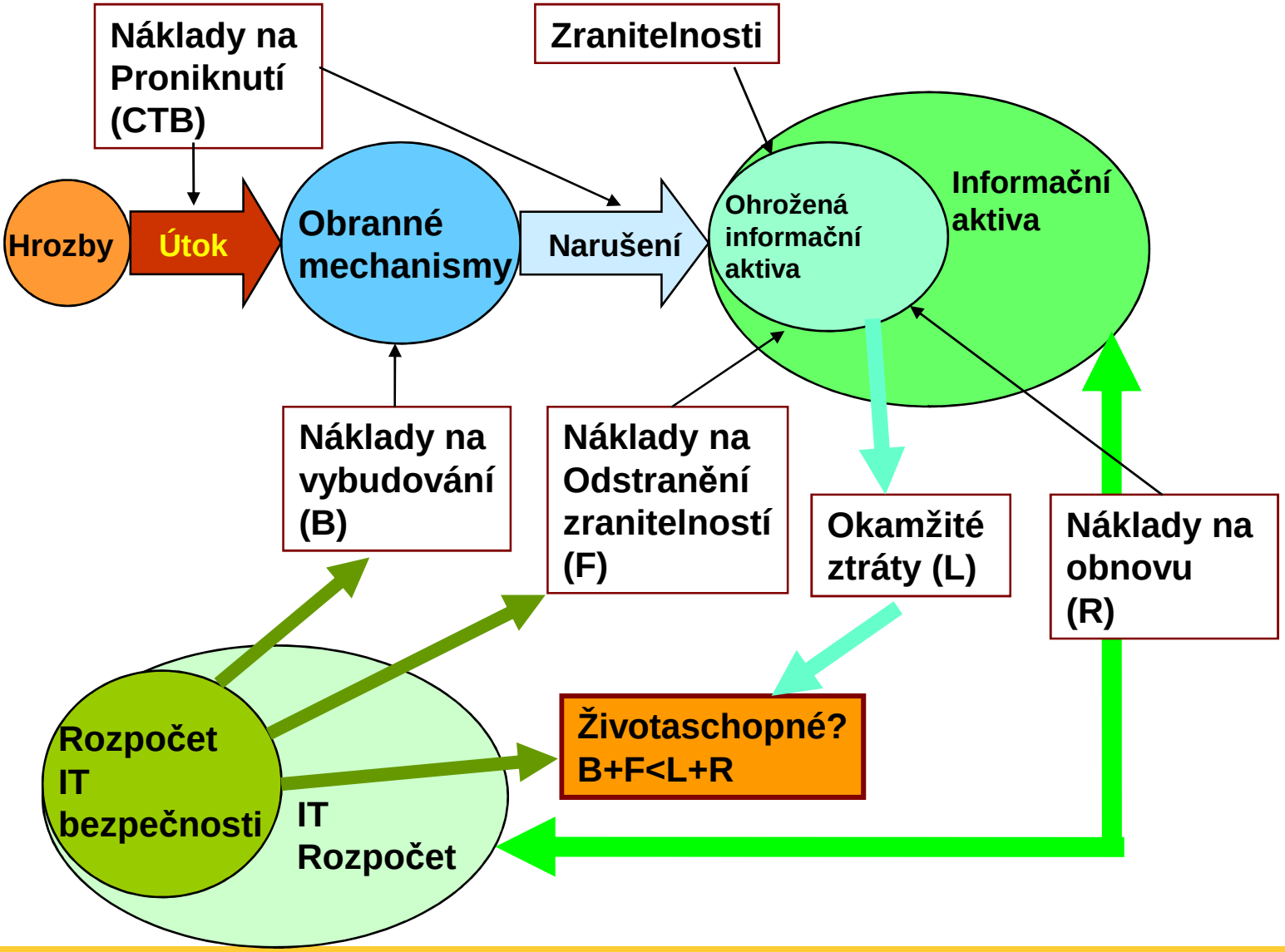
  - **CTB > (F + B + M)**

- Po vyšetřování útoků a jejich pachatelů se zjistilo, že útočník je motivován k provedení útoku, jestliže platí

  - **CTB < (Li + A(t)),**

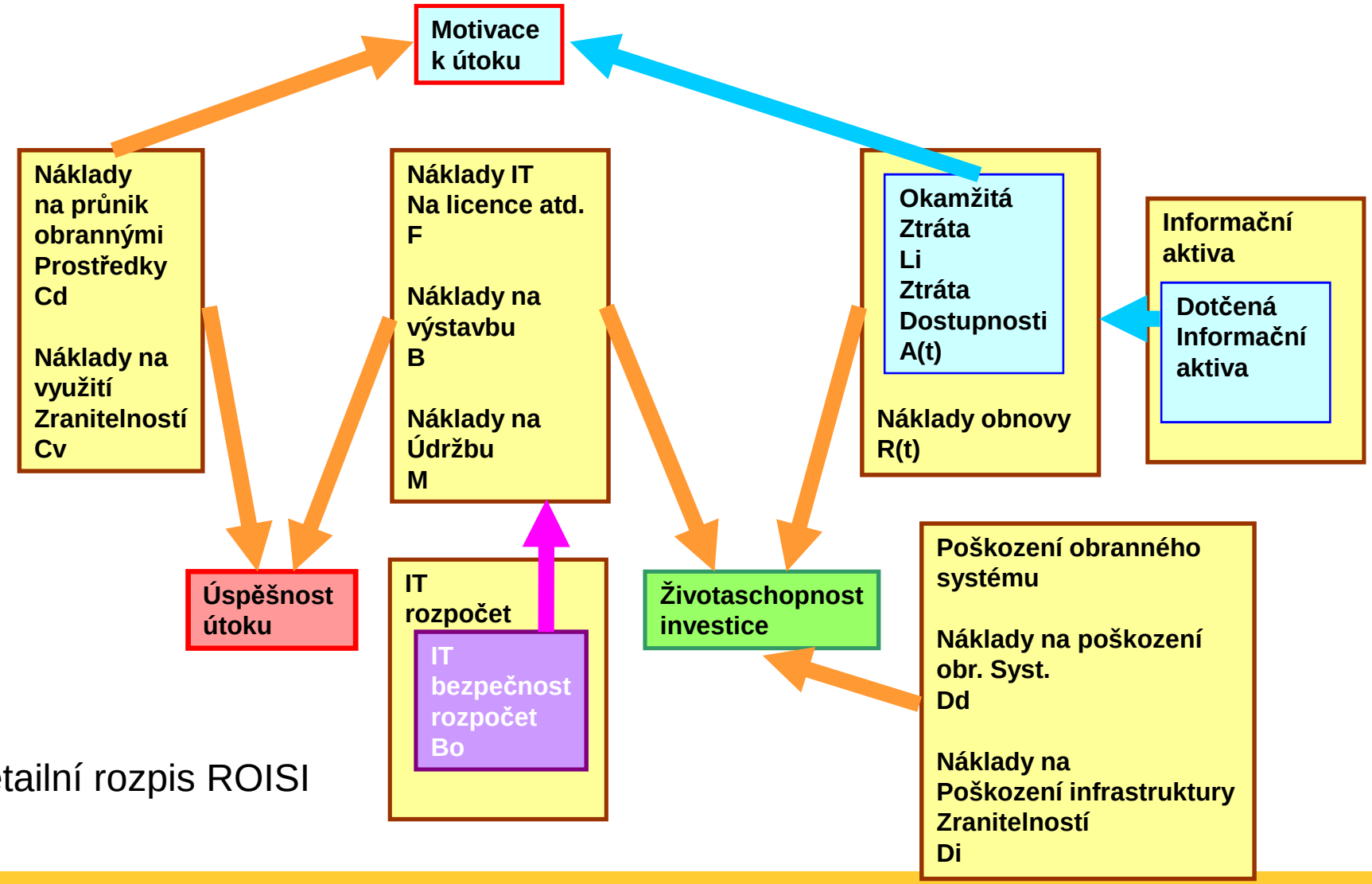
- Kde Li je okamžitá ztráta a A(t) je ztráta dostupnosti. **Pozor!** Vnímání hodnoty např. ukradených informací může být pro útočníka vyšší než pro obránce. **Platí i naopak!**

Znázornění životaschopnosti informační bezpečnosti



Zdroj: A. Mizzi, 2005, Thesis

Výpočet návratnosti investic do IB



Detailní rozpis ROISI

Závěr

- Na shledanou a ....