Opłacalność inwestycji w bezpieczeństwo systemów informatycznych (ROSI) w urzędach administracji samorządowej

Tomasz Chlebowski

ComCERT SA

21 czerwca 2013 roku

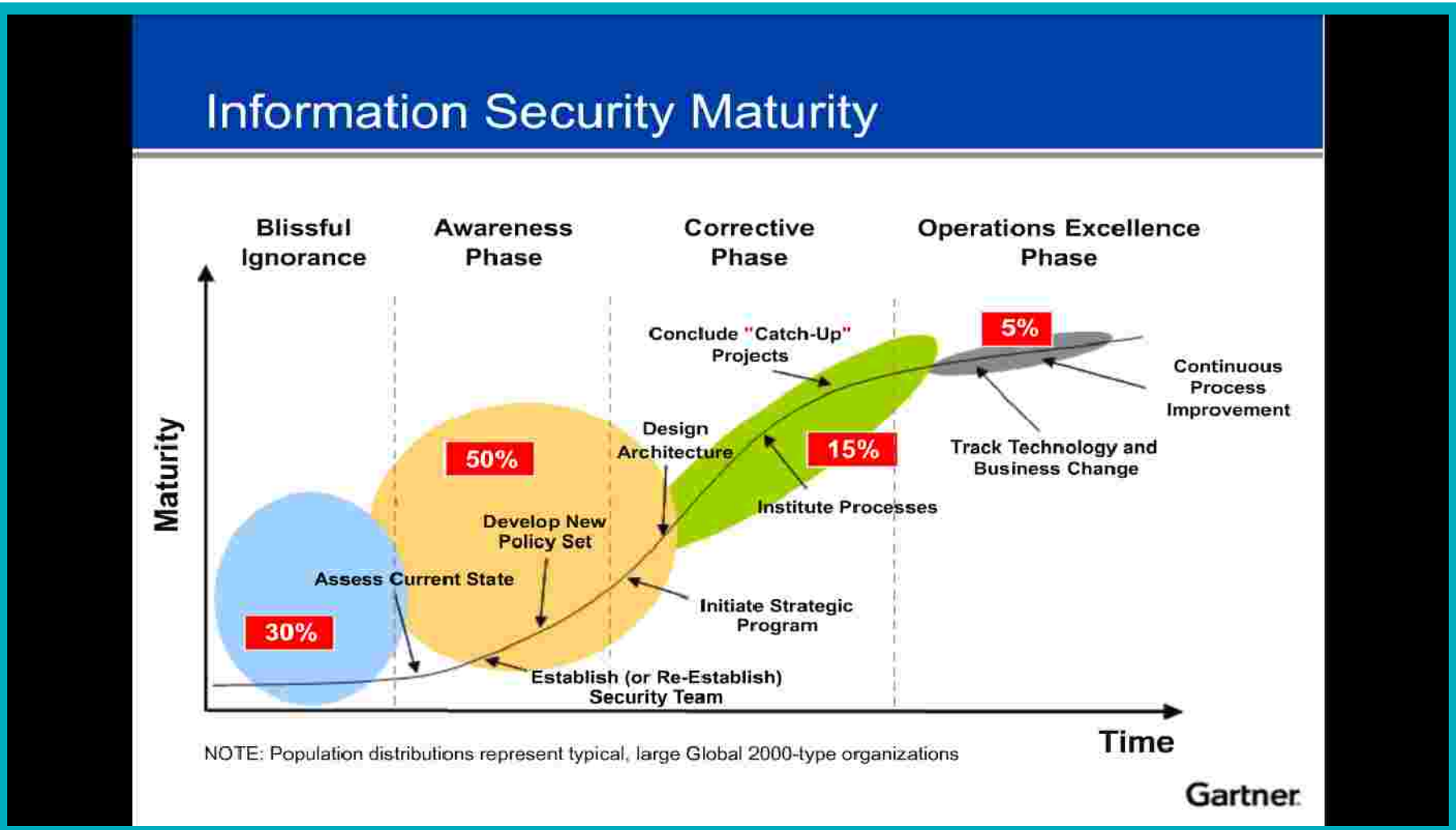
Jeden slajd o ComCERT SA

ComCERT jest jedynym niezaleznym biznesowym polskim CERT-em (Computer Emergency Response Team).

Kazda organizacja powinna nie tylko zabezpieczac sie przed wystapieniem zagrozen z sieci. Powinna równiez byc przygotowana do radzenia sobie w sytuacji, gdy takie zagrozenie mimo wszystko nastepuje. W przeciwnym przypadku kierownictwu takiej organizacji mozna zarzucic nonszalancje, brak profesjonalizmu i wyobrazni.

ComCERT pomaga organizacjom przygotowac sie do sprawnego dzialania w sytuacjach wystapienia zagrozen z cyberprzestrzeni oraz wspiera je w momencie, gdy takie zagrozenie nastapilo.

Dojrzalosc bezpieczenstwa informacji w organizacji



Odpowiedzialnosc w urzedzie

Za zapewnienie bezpieczenstwa sieciowego (informatycznego) w organizacji najczesciej odpowiedzialny jest:

- kierownik/dyrektor wydzialu informatyki, jesli podlega bezposrednio prezydentowi lub burmistrzowi czesto okreslany jest potocznie nazwa CIO (ang. Chief Information Officer) albo
- kierownik/dyrektor dzialu bezpieczenstwa informacji, jesli podlega bezposrednio prezydentowi lub burmistrzowi, czesto okreslany jest potocznie nazwa CISO (Chief Internal Security Officer)
- osoba ta czesto stoi przed dylematem, jaki budzet nalezy przedstawic przelozonemu, aby z jednej strony nie byl on nadmiarowy, a z drugiej – aby wykonac zadanie w przekonaniu, ze CIO/CISO podjal wszelkie konieczne, uzasadnione srodki w celu zapewnienia bezpieczenstwa urzedowi
- czesto stosuje sie cos w rodzaju reguly kciuka: 10% budzetu IT powinno byc przeznaczone na bezpieczenstwo IT (a 10% budzetu na bezpieczenstwo IT powinno byc przeznaczone na przygotowanie urzedu do sprawnego dzialania w sytuacji zagrozenia bezpieczenstwa)
- uzasadnienie konkretnego budzetu powinno byc zgodne z zasadami Corporate Governance. Realizacji tego zadania sluzy wykorzystanie metodyki ROSI (Return on Security Investment)

Ocena ryzyka

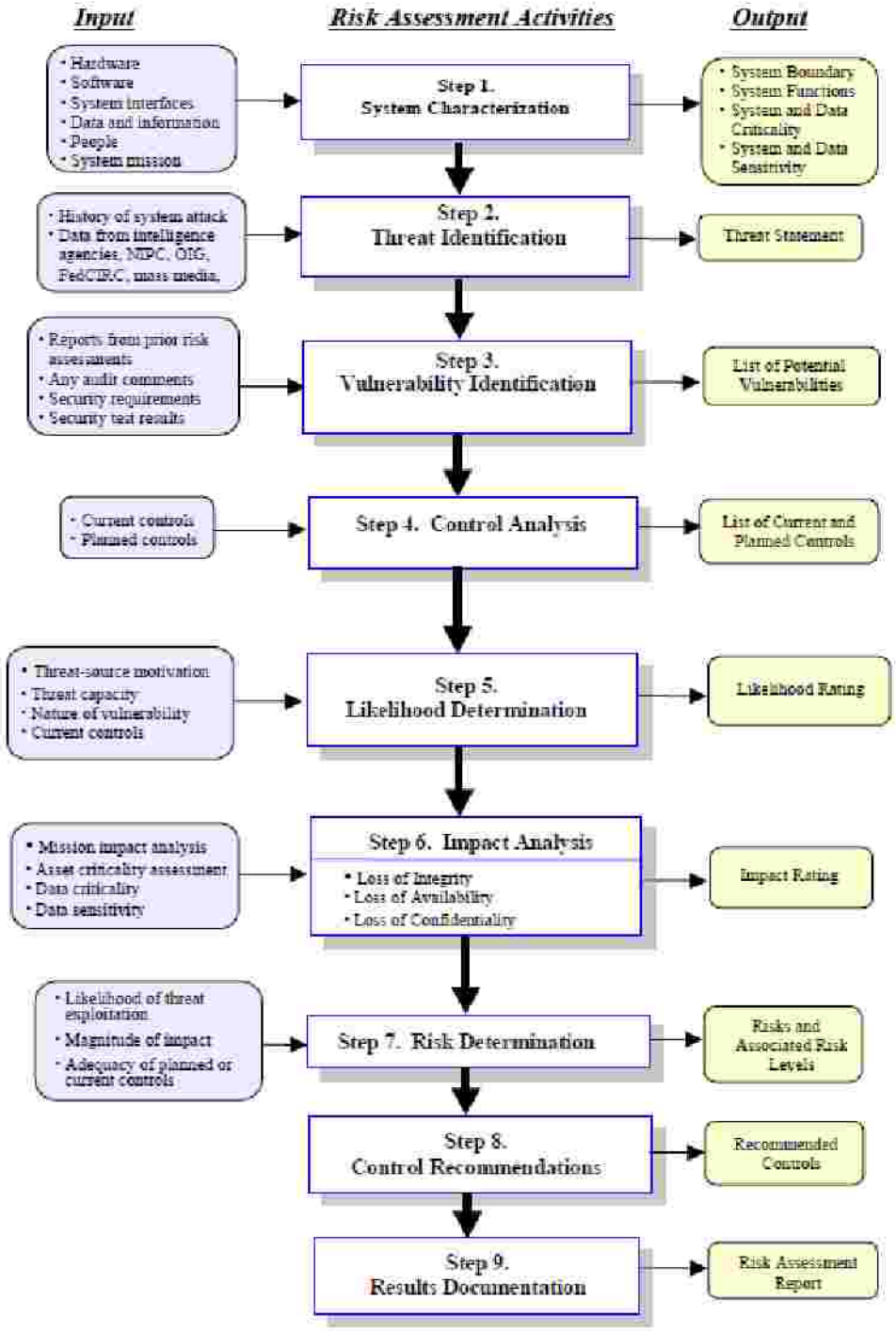
Konieczne analizy,

aby móc przeprowadzic

obliczenia

ROSI

(Return on Security Investment)



Metodyka ROSI – podstawowa Idea (1)

1. oszacowanie wielkosci strat w wyniku nastapienia kazdego (sposród róznych mozliwych) ataku (SLE – Single Loss Expectancy)
2. oszacowanie prawdopodobienstwa wystapienia ataku danego rodzaju (lub ich liczby w ciagu jednostki czasu) (ARO – Annual Rate of Occurence)
3. oszacowanie rocznego kosztu strat spowodowanych atakiem danego rodzaju (iloczyn powyzszych liczb) – (ALE Annualized Cost Expectancy)

$$ALE = SLE * ARO$$

4. suma ALE dla róznych rodzajów ataków (TALE – Total Annual Cost Expectancy)
5. rozwazenie inwestycji majacych na celu wyeliminowanie/dramatyczne zmniejszenie prawdopodobienstwa wystapienia skutecznego ataku (= powodujacego straty)
   - inwestycja o wielkosci I (skutecznie dzialajaca przez okres n lat) zmniejszy straty o X%

Metodyka ROSI – podstawowa idea (2)

ROSI – podstawowe wnioski z teorii

Najprostszy przyklad

- koszt strat w wyniku jednego ataku wirusa (SLE) wynosi 20 tys. zl
- urzad takie straty ponosi srednio 2 razy rocznie (ARO)
- jest to jedyne rozwazane zagrozenie
- inwestycja w rozwiazanie antywirusowe dla przedsiebiorstwa kosztuje 70 tys. zl (I) i gros tego kosztu to 3-letnia licencja na oprogramowanie
- skaner antywirusowy obniza prawdopodobienstwo skutecznego ataku (czyli poniesienia strat) czterokrotnie (X = ¾)
- ROSI = (20 tys. zl * 2 rocznie * ¾ * 3 lata – 70 tys. zl) / 70 tys. zl = 29%

Projekt jest opłacalny

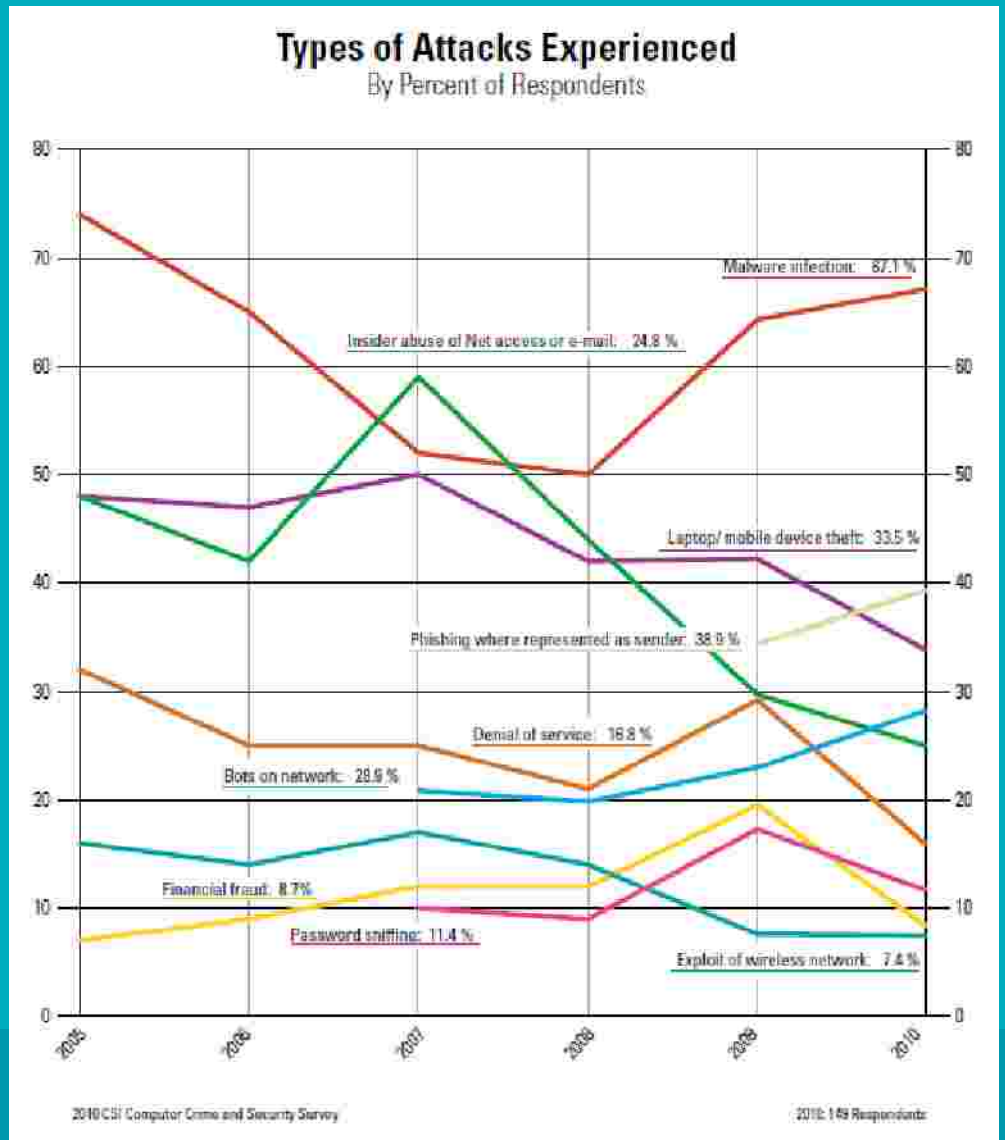
praktyka

- Problem polega na tym, ze bardzo trudno oszacowac wielkosc ponoszonych strat, a jeszcze trudniej – prawdopodobienstwo ataku.

O jakie ataki chodzi (klasyfikacja incydentów wedlug eCSIRT.net)

- Obrazliwe i nielegalne tresci:
  - spam,
  - dyskredytacja, obrazanie,
  - przemoc;
- Zlosliwe oprogramowanie:
  - wirus,
  - robak sieciowy,
  - kon trojanski,
  - oprogramowanie szpiegowskie,
  - dialer;
- Gromadzenie informacji:
  - skanowanie,
  - podsluch,
  - inzynieria spoleczna;
- Próby wlaman:
  - wykorzystanie znanych luk systemowych,
  - próby nieuprawnionego logowania,
  - wykorzystanie nieznanych luk systemów;
- Wlamania:
  - wlamanie na konto uprzywilejowane,
  - wlamanie na konto zwykle,
  - wlamanie do aplikacji;
- Atak na dostepnosc zasobów:
  - atak blokujacy serwis (DoS),
  - rozproszony atak blokujacy serwis (DDoS),
  - sabotaz komputerowy;
- Atak na bezpieczenstwo informacji:
  - nieuprawniony dostep do informacji,
  - nieuprawniona zmiana informacji;
- Oszustwa komputerowe:
  - nieuprawnione wykorzystanie zasobów,
  - naruszanie praw autorskich,
  - kradziez tozsamosci, podszycie sie (w tym phishing).

Rozklad najczestszych incydentów



Skladniki strat ponoszonych w wyniku ataku

Nie kazdy atak kosztuje zaatakowanego tyle samo, aby okreslic wielkosc strat nalezy uwzglednic m.in.:

- zasieg ataku (jakich wydzialów urzedu, lokalizacji, jednostek biznesowych, procesów dotyczyl atak), jakie czesci urzedu zostaly zaangazowane
- wartosc odtworzeniowa zniszczonych urzadzen, jesli takie byly
- koszt pracy pracowników, zarówno tych których produktywnosc zostala zmniejszona, jak i tych, którzy musieli zostac zaangazowani do minimalizowania skutków, naprawiania systemów, odtwarzania, itd.
- koszty posrednie, narzuty, itp
- koszt utraty danych poufnych/tajnych (dane osobowe, projekty, plany, ...)
- wielkosc odpowiedzialnosci prawnej lub kar umownych, których koniecznosc wyplaty spowodowal incydent
- utracona wartosc e-urzedu w oczach obywateli (utrata korzystajacych, zmniejszenie przyrostu nowych)
- spadek/utrata wizerunku urzedu.
- koszty alternatywne (utracone pieniadze urzad móglby np. zainwestowac)

STRATY (przyklady – 1)

- Nie kazdego taki sam atak kosztuje tyle samo, np. utrate notebooka jedne firmy oceniaja na 10 tys. zl (lacznie z wartoscia zawartosci, kosztem zakupu nowego, odtworzenia konfiguracji i zawartosci, czasem koszt utraty znizki ubezpieczeniowej), a inne organizacje – nawet na 300 tys. zl
- koszty pracowników (utrata produktywnosci). Jesli przykladowo atak uniemozliwia 100 pracownikom prace przez 8 godzin i srednio godzina pracy tych pracowników kosztuje Urzad (lacznie z ZUS-em, kosztem wyposazenia stanowiska, itd.) 50 zl, a ponadto 6 pracowników dzialu IT musi pracowac przez tydzien, aby usunac skutki ataku, ich godzina kosztuje 100 zl, to laczny pracowniczy koszt takiego ataku wynosi: 100 * 8 * 50 zl + 6 * 40 * 100 zl = 42 400 zl

STRATY (przyklady – 2)

- koszty spowodowane przez spam: 100 pracowników otrzymuje srednio 10 spamów dziennie i „obróbka” 1 spamu przez pracownika (którego godzina pracy kosztuje pracodawce 50 zl) trwa 10 sekund. Roczny koszt spamu wynosi wiec 100 pracowników * 220 pracujacych dni w roku * 10 sekund * 10 spamów = 611 h @ 50 zl = 31 tysiecy zl. Do tego nalezy dodac koszt urzadzen obslugujacych spam i przestrzeni dyskowej, gdzie czesc tego spamu laduje czesto niestety na dluzej (ponadto srednio co 13. spam jest zawirusowany...)
- atak DDoS na Urzad Miasta, trwajacy np. 48 godzin, nie jest natychmiast odczuwany finansowo, tak jak w przypadku np. firmy e-commerce, ale straty wynikaja z:
  - spadku zaufania obywateli do e-Urzedu
  - zla opinia o Urzedzie, a szczególnie o jego informatykach

STRATY (przyklady – 3)

- Urzedowi – w wyniku ataku – wykradziono dane dotyczace 2000 mieszkanców. Urzad zostal oskarzony o zlamanie prawa przez niedostateczne zabezpieczenie danych klientów. W wyniku przegranych procesów Urzad stracil:
  - 100 godzin pracy Prezydenta/Burmistrza i prawników @ 100 zl = 10 tys. zl
  - moze odszkodowania dla mieszkanców 2000 * 100 zl = tys. zl
  - inne koszty procesów sadowych = 20 tys. zl
  - w sumie 230 tys. zl.

- Ponadto:
  - jeden z cennych pracowników odchodzi z Urzedu (w wyniku oskarzen/dochodzen, ...) – koszty zastapienia – 20 tys. zl

- Lacznie 250 tys. zl

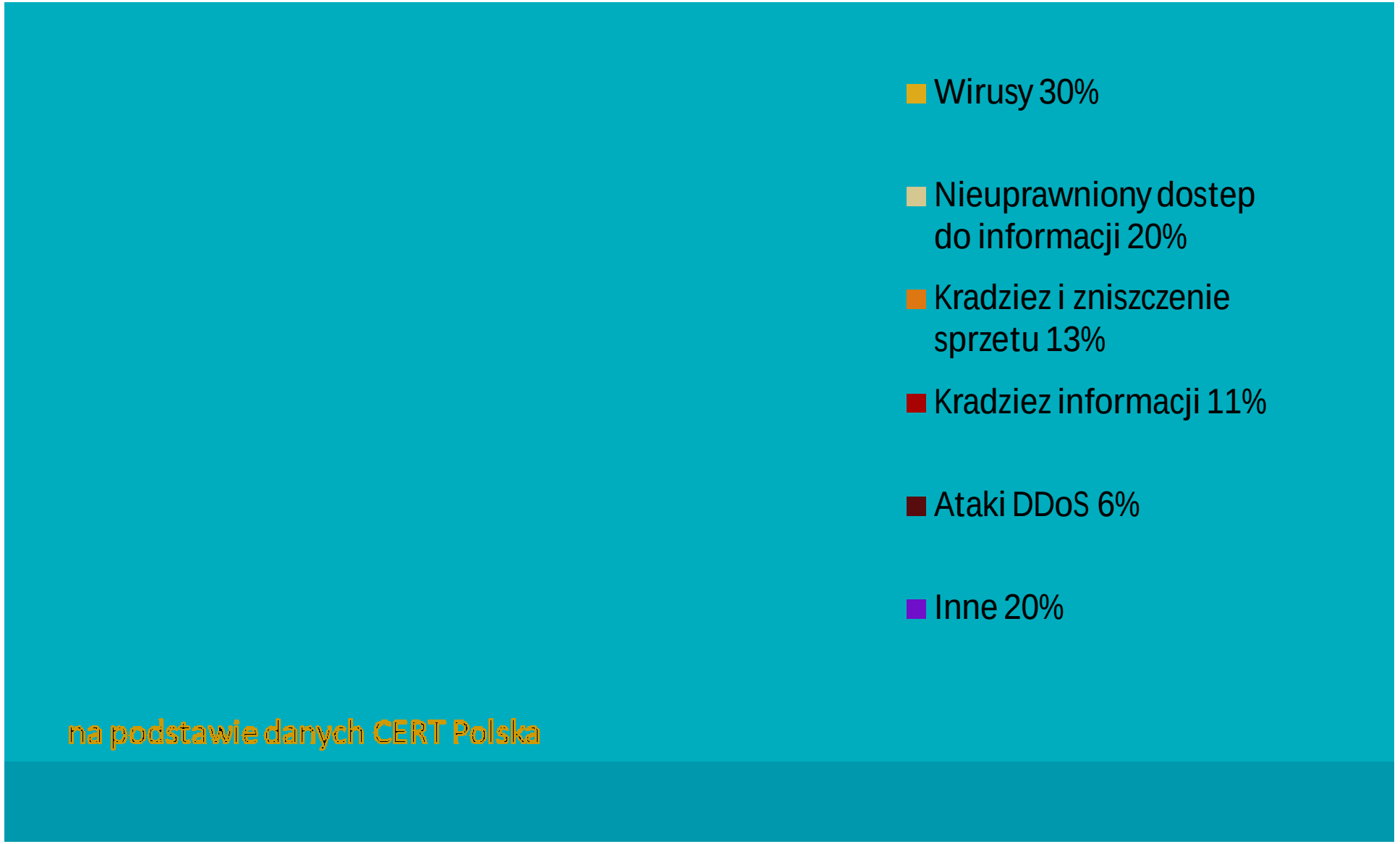
STRATY (Przyklady – 4)

- Jeden z komputerów Urzedu (jako Zombie, bez swiadomosci kogokolwiek w Urzedu) rozsylal tresci nielegalne. W wyniku przeszukania przez CBS zarekwirowano (jako dowód w sprawie) komputery 3 pracowników i administratora.
- Koszty:
  - 100 pracowników nie pracowalo przez 8 h (koszt = 40 000 zl) w czasie wizyty CBS
  - 3 pracowników stracilo wyniki miesiecznej pracy (25 000 zl)
  - trzeba bylo kupic te komputery, bo na ich odzyskanie przed zakonczeniem sprawy nie ma co liczyc (20 000 zl)
  - opublikowano w prasie informacje o rozsylaniu tresci przez Urzad, co narazilo na strate reputacji Urzedu i Burmistrza...
    - Lacznie co najmniej 100 tys. zl

STRATY - Podsumowanie

W kazdym z powyzszych przykladów straty Urzedu w wyniku wystapienia 1 ataku/incydentu liczone sa czesto w setkach tysiecy zlotych, a nawet moga doprowadzic do oskarzenia Prezydenta/Burmistrza o niefrasobliwosc

Najkosztowniejsze incydenty



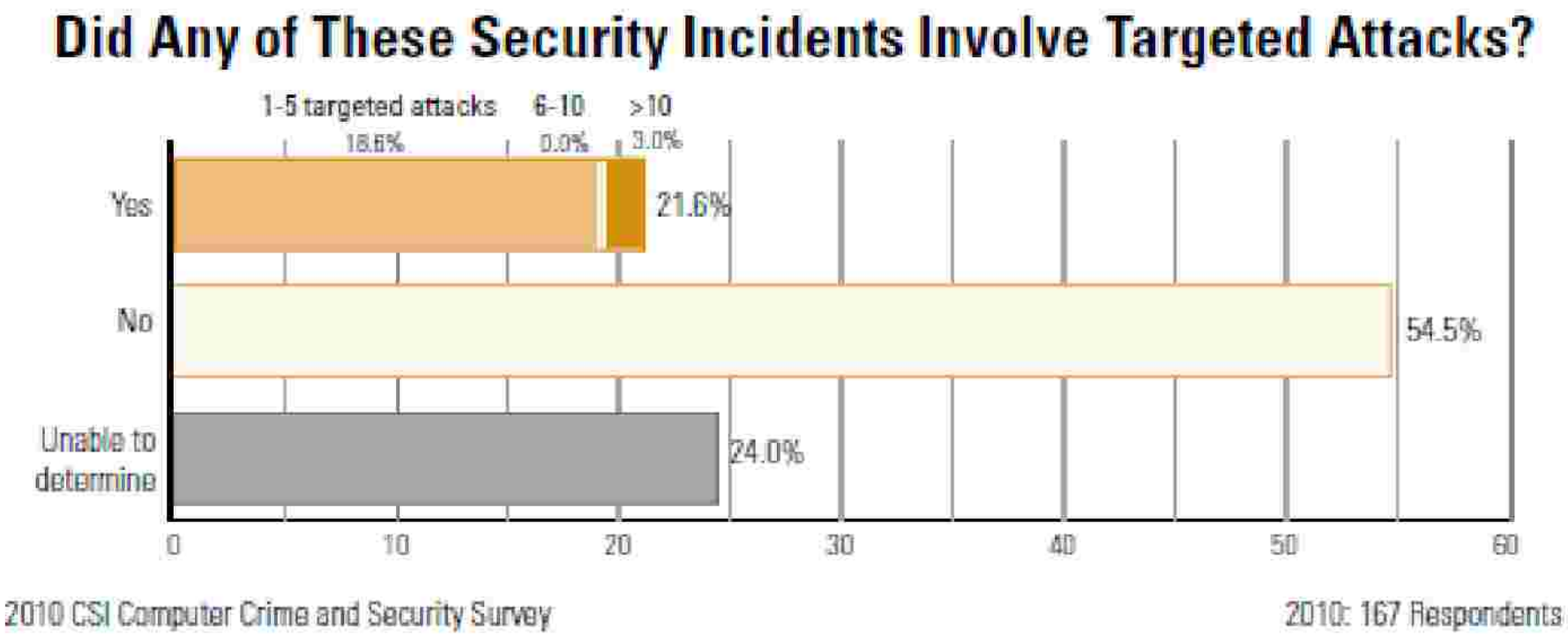
na podstawie danych CERT Polska

Oszacowanie czestotliwosci (ARO)

Nie w kazdym rodzaju incydentów oszacowanie czestotliwosci jest trudne. Trywialna zasada: im czestsze incydenty, tym latwiej okreslic prawdopodobienstwo ich wystapienia. Przykladowo:

- w przypadku spamu – kazdy dostaje go tyle, ze bardzo latwe jest oszacowanie wielkosci strat
- ataki, które zdarzaly sie w Urzedzie (lub zaprzyjaznionych instytucjach w przeszlosci (w liczbie wiekszej niz 1) równiez daja podstawe do oszacowania czestotliwosci. Niektóre dane mozna uzyskac od CERT-ów (np. ComCERT-u)
- najtrudniej oszacowac zdarzenia, które dotychczas nie wystapily w Urzedzie. Szacunki nalezy oprzec na danych zewnetrzn ch, ale adekwatnych do warunków i zagrozen danej instytucji.

Czestotliwosc i rodzaj ataków



Oszacowanie stopnia redukcji ryzyka (X)

- poprawnie zaimplementowane rozwiazanie powinno pozwalac na calkowite usuniecie niebezpieczenstwa (X = 100%)
- w literaturze przyjmuje sie konserwatywnie X = 85%

ale

- czesto zabezpieczenie jest tylko czesciowe (np. „drzwi pancerne, a obok okno”), wtedy X = 0
- zdarza sie, ze pelne zabezpieczenie powoduje paraliz biznesu, wtedy konieczne sa rozwiazania kompromisowe, w których swiadomie X < 100%
- X czesto maleje z czasem, poniewaz hackerzy ucza sie omijania zabezpieczen

Spojrzenie strategiczne

- Znajac (lub lepiej lub gorzej szacujac) wszystkie elementy mozemy policzyc ROSI, który odpowiada ogólniejszemu pojeciu ROI zastosowanego do tematu bezpieczenstwa.
- Mozna liczyc równiez inne parametry, takie jak NPV (Net Present Value) albo IRR (Internal Rate of Return). Metodyka wyliczania kazdego z tych parametrów wrazliwa jest na inne aspekty analizy. Przykladowo rozwazmy 2 przypadki:

Przypadek	Koszt urzadzenia	NPV	IRR	ROSI
1	100	358	400%	400%
2	100	278	38%	400%

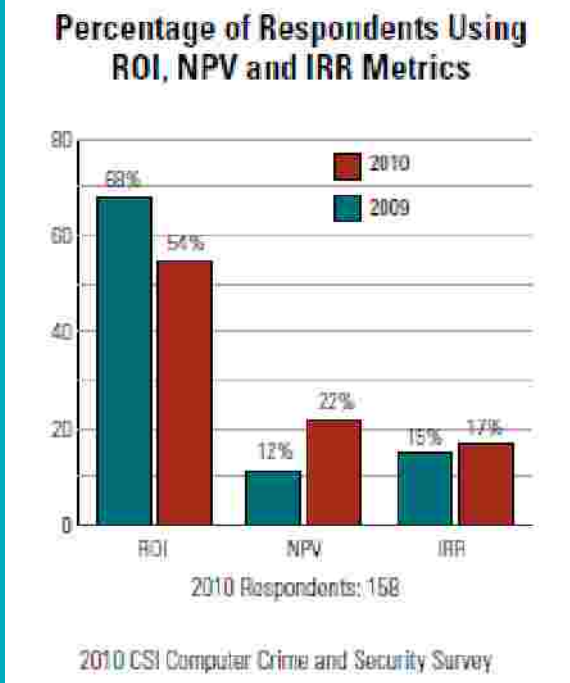
1. zakup urzadzenia za 100 tys. zl pozwolilo na unikniecie strat w wysokosci 500 tys. zl juz w pierwszym roku jego dzialania
2. zakup tego samego urzadzenia pozwolilo na unikniecie powyzszej straty w piatym roku jego pracy (w tabeli wszystkie liczby sa w tysiacach zlotych)

Oszacowania (w tys. zl)

Poniewaz nie wiemy z góry, kiedy atak moze nastapic, w szacowaniu parametrów mozna:

1. spodziewane unikniecie strat w wyniku inwestycji rozlozyc równomiernie w czasie, albo
2. rozlozyc w czasie tak, aby uwzglednic najwieksza wartosc X w pierwszym okresie stosowania zabezpieczenia i malejaca jego wartosc w czasie.

W tych przypadkach oczekiwane ROSI, NPV i IRR wyniosa (w tys. zl)



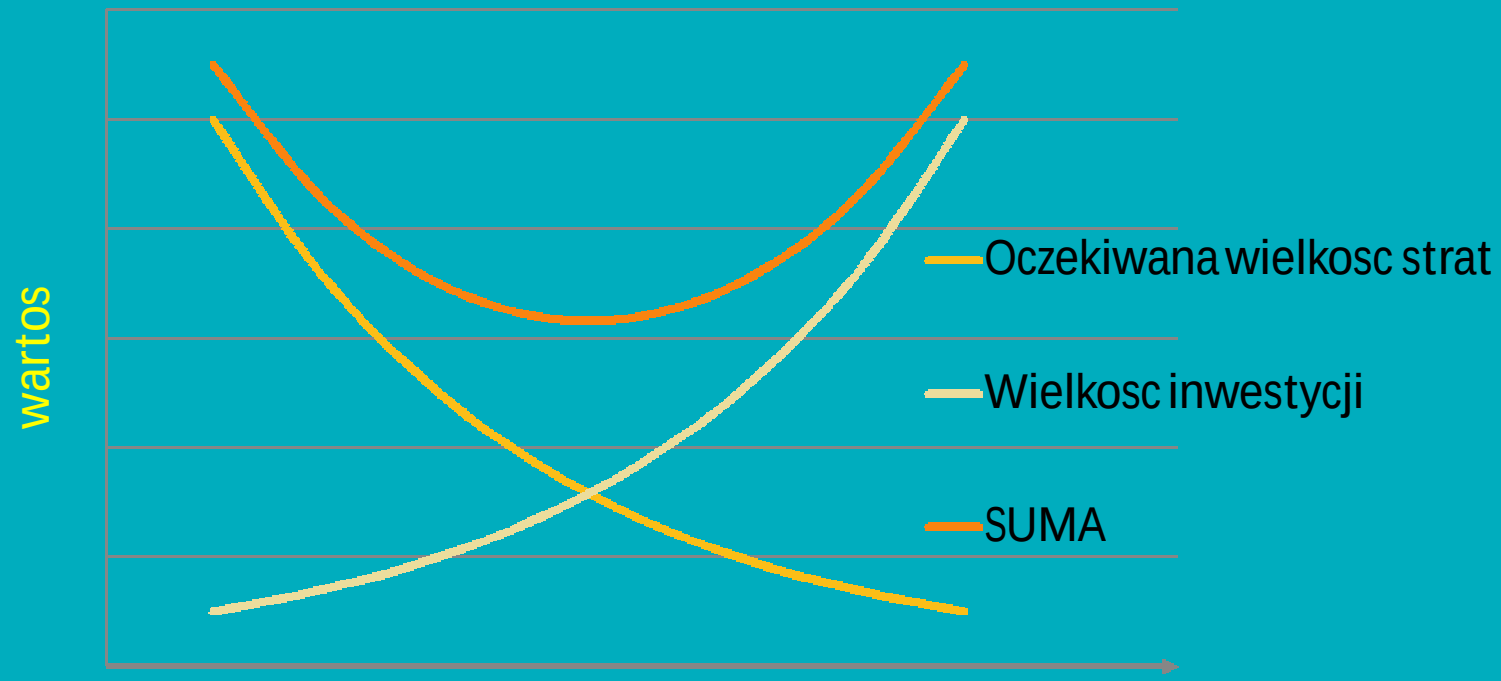
Przypadek	Koszt urzadzenia	NPV	IRR	ROSI
1	100	317	97%	400%
2	100	333	153%	400%

Kalkulacje ROSI (w oparciu o NPV)

w tys. zl

nr	krok	Opcje			
		A	B	C	D
1	Inwestycja w bezpieczenstwo (w czasie t=0)	0	65	130	195
2	Wlk. straty w przyp. ataku (bez inw., t=1)	1000	1000	1000	1000
3	Prawdop. straty przy inwestycji, jak w wierszu 1	75%	50%	40%	33%
4	Wielkosc oczekiwana straty (w t=1)	750	500	400	330
5	Dzisiejsza oczekiwana wartosc straty (w t=0)	652	435	348	287
6	Oczekiwany koszt calkowity (strata+inwestycja), w czasie t=0	652	500	478	482
7	Przyrost korzysci z inwestycji	n/d	152	22	-4

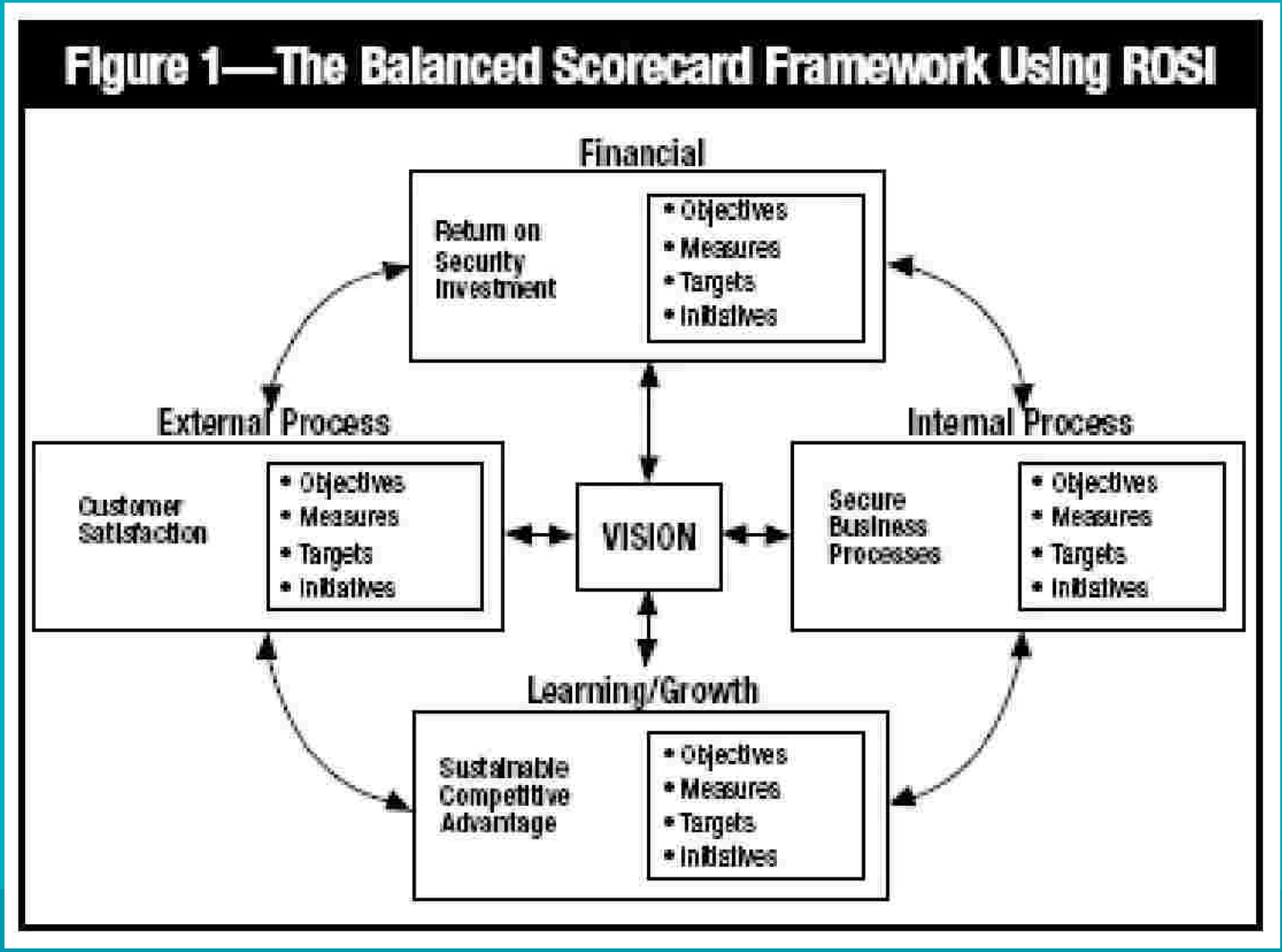
Optymalna wielkosc inwestycji w bezpieczenstwo



Ryzyko = wielkosc iloczynu prawdopodobienstwa zdarzenia i wielkosci pojedynczej straty

Zastosowanie ROSI przy strategicznym zarzadzaniu organizacja

ISACA
Serving IT Governance Professionals



Krytyka ROSI i odpowiedz

- jest bardzo trudno oszacowac zarówno prawdopodobienstwo ataku, jak i wielkosc poniesionych strat (z góry), ale czy lepiej jest nie robic nic niz spróbowac oszacowac koniecznosc niezbednych inwestycji w najlepszy – sposród niedoskonalych – sposób?

- Takie wlasnie podejscie zapewnia metodyka ROSI

Podsumowanie

- Metoda ROSI jest waznym narzedziem pracy CIO/CISO w szacowaniu koniecznych inwestycji w bezpieczenstwo przedsiebiorstwa
- Jest to najprostsza metoda, która pozwala na udowodnienie oplacalnosci koniecznych inwestycji w bezpieczenstwo Urzedu
- Na jej podstawie mozna budowac bardziej skomplikowane modele ekonomiczne, jednak ze wzgledu na nieznajomosc momentu nastapienia ataku, metody uwzgledniajace wartosc pieniadza w czasie nie daja bardziej wiarygodnych wyników niz ROSI.
- ComCERT S.A. jest spólka specjalizujaca sie we wsparciu Urzedów przy projektowaniu optymalnych inwestycji w bezpieczenstwo.

Dziekuje

Tomasz Chlebowski

tomasz.chlebowski@comcert.pl