**Evaluarea RI după ROSI a Băncii MAIB**



|  |  |
| --- | --- |
| Code: |  |
| Version: | 1.1 |
| Date of version: | 12.01.2023 |
| Created by: | Cebotari Dan |
| Approved by: | lect. univ. Bulai Rodica |
| Confidentiality level: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 15.12.2022 | 1.0 | Cebotari Dan | Schița de bază a documentului |
| 12.01.2023 | 1.1 | Cebotari Dan | Schița de bază a documentului |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[SCOPUL ȘI DESCRIEREA OBIECTIVELOR 3](#_Toc124429647)

[TERMINOLOGIA DE BAZĂ 3](#_Toc124429648)

[FORMULE DE BAZĂ 4](#_Toc124429649)

[EXEMPLU CALCUL MANUAL ROSI 4](#_Toc124429650)

[PREZENTARE CALCULATOR ADVISERA ROSI 5](#_Toc124429651)

[REZULTATE CALCULATOR ADVISERA ROSI 5](#_Toc124429652)

[CONCLUZIE 6](#_Toc124429653)

[ANEXA 6](#_Toc124429654)

[Chestionarul ADVISERA 6](#_Toc124429655)

# SCOPUL ȘI DESCRIEREA OBIECTIVELOR

Scopul acestui document este calculul rentabilității investiției de securitate (ROSI).

Capacitatea de a măsura performanța este în centrul oricărui management eficient, iar măsurarea performanței este esențială pentru a aloca resurse, selecta operațiuni și recompensa personalul.

Investițiile în IT-Security sunt vitale pentru companii. Măsurarea valorii anumitor activități pentru îmbunătățirea securității este dificilă, din cauza consecințelor în principal invizibile ale deciziilor. Abordările tradiționale pentru sprijinirea deciziilor au deficiențe importante.

Analiștii încercă să identifice posibilele riscuri și daune și apariția probabilă a atacurilor cibernetice pentru a nu rata investițiile necesare în securitate. Cu toate acestea, aceste riscuri și probabilități sunt greu de luat în considerare. Măsuri există, dar indiferent de rentabilitatea investiției în securitate (ROSI) este necesar să încercăm să evaluăm calitatea investiției.

# TERMINOLOGIA DE BAZĂ

Confidențialitate – caracteristică a informațiilor prin care acestea sunt disponibile numai persoanelor sau sistemelor autorizate.

Integritate – caracteristică a informațiilor prin care acestea sunt modificate numai de către persoane sau sisteme autorizate într-un mod permis.

Disponibilitate – caracteristică a informațiilor prin care poate fi accesată de către persoanele autorizate atunci când este nevoie.

Securitatea informațională – garantarea confidențialității, integrității și disponibilității informațiilor.

ROSI (Return on Security Investment) – valoarea monetară a investiției este comparată cu valoarea monetară a reducerii riscului.

SLE (Single Loss Expectancy) – valuarea pagubei, costul total al unui incident, presupunând apariția sa unică.

ARO (Annual Rate of Occurrence) – rata anuală de apariție a riscurilor, o măsură a probabilității ca un risc să apară într-un an.

ALE (Annual Loss Expectancy) - pierderea monetară anuală care poate fi așteptată de la un anumit risc pe un anume activ.

Risk - o măsură a măsurii în care o entitate este amenințată de o potențială circumstanță sau eveniment și, de obicei, o funcție a impacturilor negative care ar apărea dacă circumstanța sau evenimentul ar avea loc și probabilitatea de apariție.

Vulnerabilitate - slăbiciunea unui sistem informațional, proceduri de securitate a sistemului, controale interne sau implementare care ar putea fi exploatate sau declanșate de o sursă de amenințare.

Risk Assessment - procesul de identificare a riscurilor pentru operațiunile organizaționale, activele organizaționale, indivizii, face parte din managementul riscurilor, încorporează analize de amenințări și vulnerabilități și ia în considerare atenuările oferite de controalele de securitate planificate sau în vigoare.

# FORMULE DE BAZĂ

După definiția ROI, ROSI este definit după cum urmează:

Implementarea unei soluții de securitate eficace scade ALE: cu cât o soluție este mai eficientă,cu atât ALE este mai redusă. Această reducere a pierderilor monetare poate fi definită prin diferența de ALE fără soluția de securitate față de ALE modificată (mALE) care implementează soluție de securitate.

Care este, de asemenea, egal cu raportul de atenuare al soluției aplicate ALE:

# EXEMPLU CALCUL MANUAL ROSI

În fiecare an Banca MAIB suferă 2 atacuri de viruși, adică avem ARO = 2. S-a estimat că fiecare atac costă aproximativ 1 300$ lei, SLE = 1 300$. Această sumă a fost calculată luând în considerare pierderile de date, lucrul angajaților peste program, pentru recuperare și productivitatea în continuare a companiei.

Ca soluție este luată în calcul cumpărarea unei noi soluții Antivirus. Ca obțiune este o bună alegere soluția Antivirus Bitdefender Gravityzone Business Security. Antivirusul va diminua situația cu 75% (mitigation ratio = 75%), și va costa 300$.

Antivirusul oferă următoarele privilegii:

* controale de securitate premium care pot fi personalizate pentru a răspunde nevoilor diferitelor utilizatori;
* implementare software de la distanță simplă și eficientă pe toate computerele neprotejate;
* reglementarea accesului angajaților la anumite aplicații și site-uri web pentru a îmbunătățirea productivității afacerii;
* software-ul oferă mai multe straturi de protecție de securitate pentru diferite puncte finale, cum ar fi servere, laptopuri și desktop-uri;

Soluția Antivirus ar trebui să blocheze și să prevină 85% din atacuri, rezultă raportul de atenuare este de 85%.

Conform calculului ROSI, această suluție antivirus este cost-efectivă.

# PREZENTARE CALCULATOR ADVISERA ROSI

**Free Return on Security Investment Calculator**

<https://advisera.com/27001academy/free-tools/free-return-security-investment-calculator/>

Calculatorul Free Return on Security Investment Calculator este o soluție pentru situația în care măsurile de sucuritate sunt prea scumpe, sau este greu de explicat conducerii companiei că ar putea fi consecințe în cazul în care apare un incident. Calculatorul este complet gratuit.Prin urmare, o investiție în securitate este considerată a fi profitabilă dacă efectul de diminuare a riscului este mai mare decât costurile așteptate.

Urmând această definiție, iată cum calculul ROSI efectuează analiza rentabilității investiției în securitate:

Pasul #1 – calculează costul unui incident luând în considerare toate costurile relevante dacă are loc un incident și probabilitatea apariției incidentului.

Pasul #2 – calculează costul măsurilor/controlelor de securitate și nivelul la care riscul acestui incident ar scădea din cauza unei astfel de atenuări.

Rezultatul final (după Pasul #2) este calculul dacă câștigul (scăderea riscului) este mai mare decât investiția necesară (măsuri de securitate/controale).

# REZULTATE CALCULATOR ADVISERA ROSI



**ROSI** pozitiv indică măsura de securitate profitabilă(323,28%).

# CONCLUZIE

În fiecare organizație publică sau privată, fiecare investiție bugetară trebuie să fie justificată și eficacitatea acesteia este adesea evaluată ulterior. În finanțe, această evaluare se numește Rentabilitatea Investiției sau Rata Rentabilității.

Aplicat la securitate, un calcul de Rentabilitate a Investiției în Securitate (ROSI) a oferit răspunsuri cantitative la întrebări financiare esențiale precum: banca plătește prea mult pentru securitatea sa? ce impact financiar asupra productivității are lipsa de securitate? când este suficientă investiția în securitate? este acest produs de securitate benefic?

Alocarea timpului pentru a calcula ROSI înainte de a face investiții și calcularea regulată a acestuia pentru investițiile existente poate oferi mai multe beneficii. Calculat cu precizie, ROSI oferă datele acționabile și fiabile de care avem nevoie pentru a ne da seama dacă eforturile sprijină într-adevăr strategia de securitate IT și reduce riscurile cibernetice, pentru a determina dacă cheltuielile curente de securitate sunt justificate, pentru a ajusta bugetul prin realocarea resurselor către problemele prioritare, sau solicita investitii suplimentare.

În urma calculului manul și cel oferit de calculatorul Advisera, ajungem la concluzia că investițiile ce țin de securitatea informațională sunt benefice și justificate, fiindcă ne vor economisi nu doar investiții monetare, dar și ne vor proteja de pierderea datelor, lucru suplimentar al angajaților, dar și reputația băncii MAIB.

# ANEXA

## Chestionarul ADVISERA

Q. Select your industry:  
R. Banking, Other financial services  
  
Q. Type of incident:  
R. System errors/malfunctions  
  
Q. Short description of potential incident:  
R. Ransomware, malicious code.  
  
Q. Existing security measures:  
R. Backup Data,Systems And Software Updated  
  
Q. How long would the negative impacts of this incident last?  
R. 2-12 months  
  
Q. Locations and business units that would be affected with this incident:  
R. Human Resources,Data Security, IT Departament  
  
Q. Business processes that would be affected by this incident:  
R. All business processes

Q. Data that would be affected by the incident:  
R. databases, software, documents  
  
Q. Physical assets that would be affected by the incident:  
R. hardware  
  
Q. Currency  
R. USD - US Dollar  
  
Q. Cost of external services:  
R. 1000  
  
Q. Cost of purchasing equipment/goods/materials  
R. 300  
  
Q. Employee costs of resolving the incident  
R. 30  
  
Q. Legal and/or contractual penalties  
R. 0  
  
Q. Description of other costs not mentioned above  
R.  
  
Q. Amount of other costs  
R.  
  
Q. Average margin in your revenues (% of your revenues)  
R. 1  
  
Q. Lost revenues from existing clients  
R. 0  
  
Q. Lost revenues from potential clients  
R. 0  
  
Q. Insurance claims  
R. 0  
  
Q. Total cost of single incident = Single Loss Expectancy (SLE)  
R. 1330.00  
  
Q. How often could such an incident occur  
R. Once a year

Q. One year risk exposure to this incident = Annualized Loss Expectancy (ALE)  
R. 1330.00  
  
  
Q. Description of security measure(s)  
R. Backup Data, Installed Antivirus Software & Firewalls  
  
Q. Incident frequency after security measure(s) are applied  
R. Once in 5 years  
  
Q. % of reduction of Total cost of single incident  
R. 75  
  
Q. Purchase value of security measure(s)  
R. 300  
  
Q. How many years would this/these security measure(s) be used?  
R. 5  
  
Q. Value of security measure(s) after their usage  
R. 20  
  
Q. Annual cost of external parties needed for security measure(s)  
R. 100  
  
Q. Annual number of employee's man-days required for security measure(s)  
R. 50  
  
Q. Average annual cost of one employee  
R. 60  
  
Q. Number of annual working days for one employee  
R. 250  
  
Q. Description of other costs of protection not mentioned above  
R.  
  
Q. Annual amount of other protection costs  
R. 0  
  
Q. Annual cost of protection of this/these security measure(s)  
R. 252.00  
  
  
Q. Total cost of single incident (SLE) - after security measure(s) have been applied  
R. 1316.70  
Q. One year risk exposure to this incident (ALE) - after security measure(s) have been applied  
R. 263.34  
  
Q. Risk reduction  
R. 1066.66  
  
Q. Return on Security Investment (ROSI) - in absolute amount  
R. 814.66  
  
Q. Return on Security Investment (ROSI) - as percentage of protection costs  
R. 323.28