SECAdvisor: A Tool for Cybersecurity Planning using Economic Models

Muriel F. Franco[12], Christian Omlin[2], Oliver Kamer[2], Eder J. Scheid[12], Lisandro Z. Granville[1], Burkhard Stiller[2]

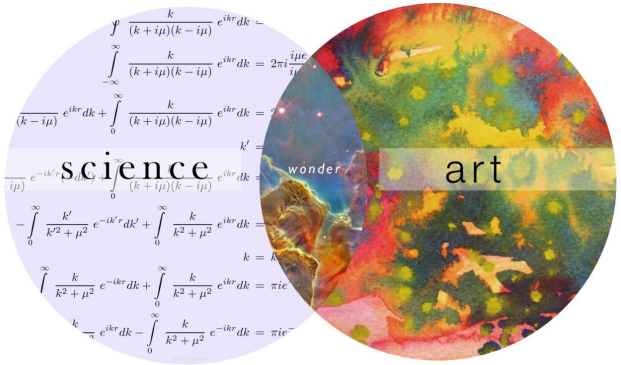
[1]Federal University of Rio Grande do Sul (UFRGS)
[2]University of Zurich (UZH)

Motivation (1)

- Risks and impacts are hard to quantify and communicate
  - 5 critical CVEs with CVSS score 9 or 20 CVEs with CVSS score 5?
  - Measurable facts (and models) can support towards Science
- How to prioritize investments?
- How to measure the effectiveness of a security control?

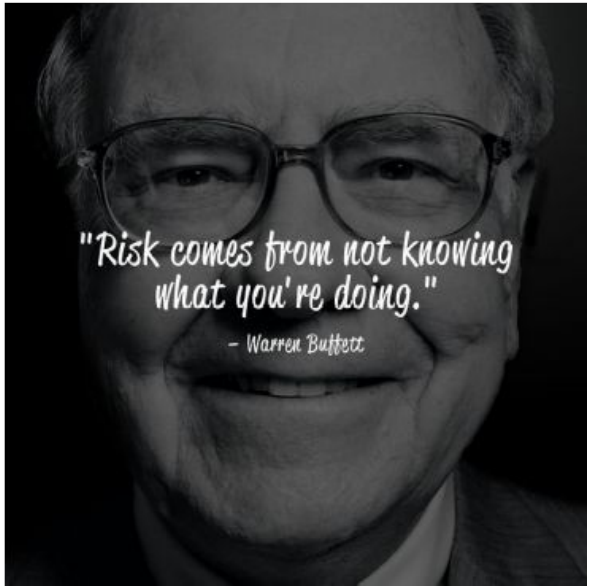
Technically but also from the Economic perspective

"Currently Cybersecurity is more Art than Science"



Travis McPeak: Hard Truths your CISO Won't Tell You. Black Hat Campfire Stories 2024

Motivation (2)



Problem

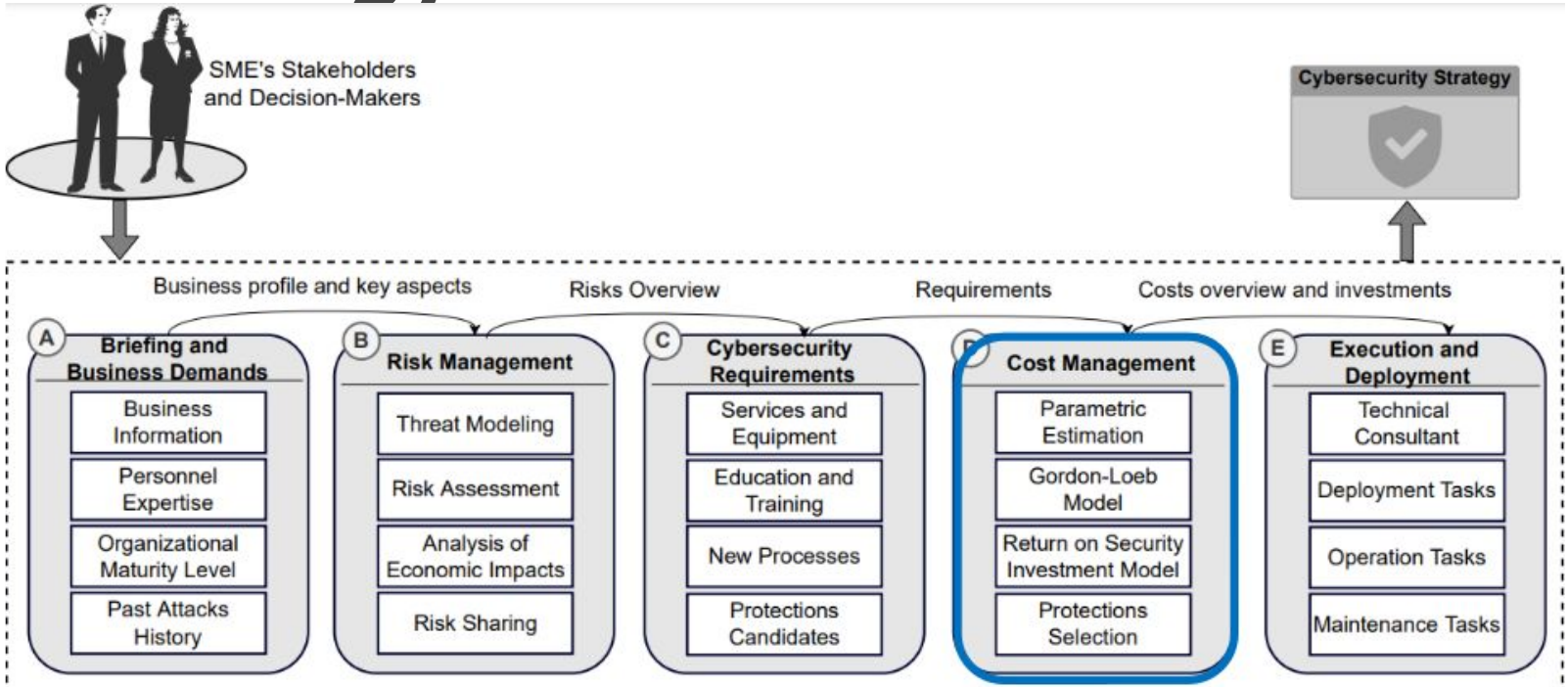
- More investments does not mean better security
  - Security increases in a decreasing rate
  - Residual risks and costs, information asymmetry
- SECAdvisor comes as a tool that implements cost management for cybersecurity planning under economic perspective

- Threats
- Risks
- Protections

- Budget
- Economic impacts

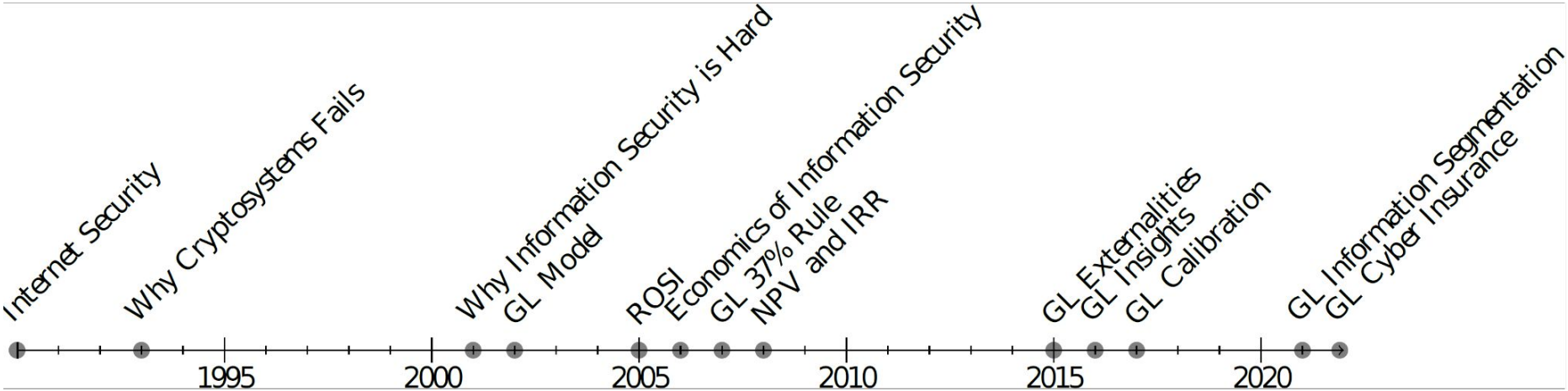
Balance betwen technical and economic

Methodology



M. F. Franco, L. Z. Granville, B. Stiller: CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment; 36th IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), Dissertation Digest, Miami, USA, May 2023.

Cybersecurity Economics in a Nutshell



M. F. Franco: CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment; PhD Thesis, University of Zurich, February 2023.

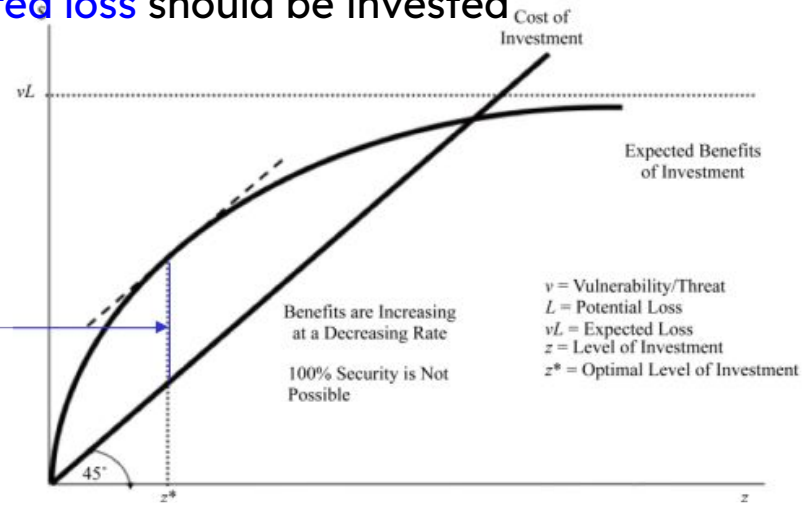
Example: Gordon-Loeb

- Economic model to analyze which is the optimal investment level in cybersecurity
  - Vulnerability of a system and the potential financial loss due to a cyberattack
  - Only a small fraction of the expected loss should be invested

$$EBIS(z) = [v - S(z, v)] * L$$

$$ENBIS = EBIS(z) - z$$

The goal is to maximize the ENBIS

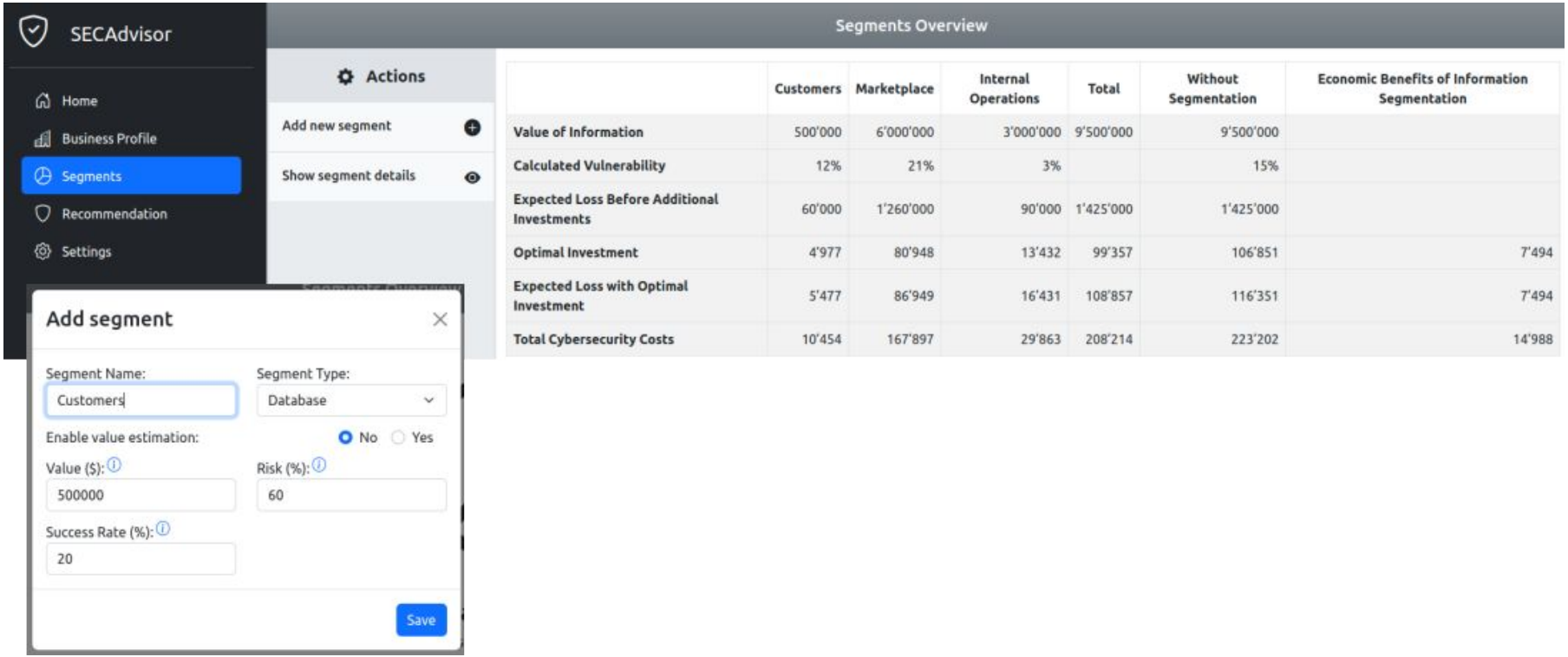


EBIS: Expected Benefit of Investment in Information Security
ENBIS: Expected Net Benefit of Investment in Information Security

Our Proposal: The SECAdvisor Tool

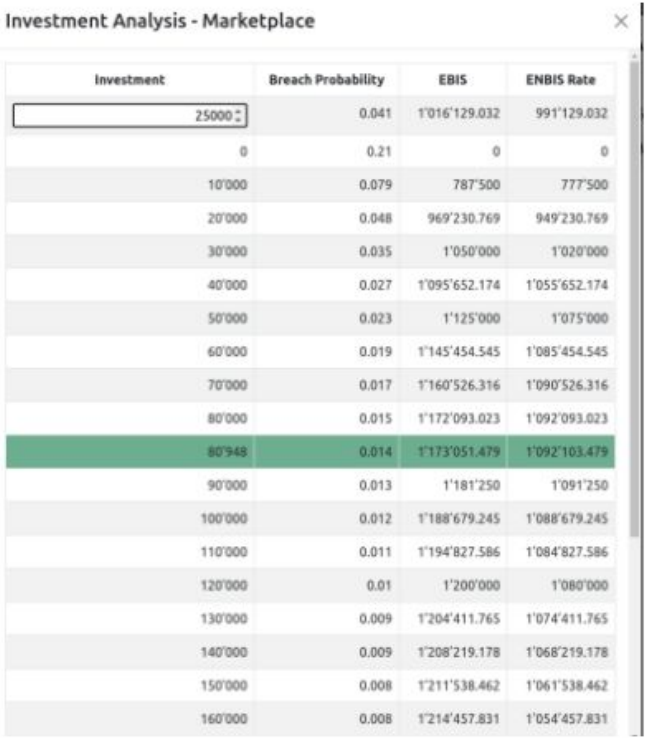
- Support the decision on how to invest in cybersecurity and understand potential losses within integrated tool
- Visual tool that provides insights about investments per segments and recommends cost-effective solutions
- **SECAdvisor Approach:**
  - Information segmentation and assets valuation
  - Gordon-Loeb model applied for investment decision
    - Customization of security breach probability functions
  - Return On Security Investment metric, recommendation

SECAdvisor - Economic Analysis



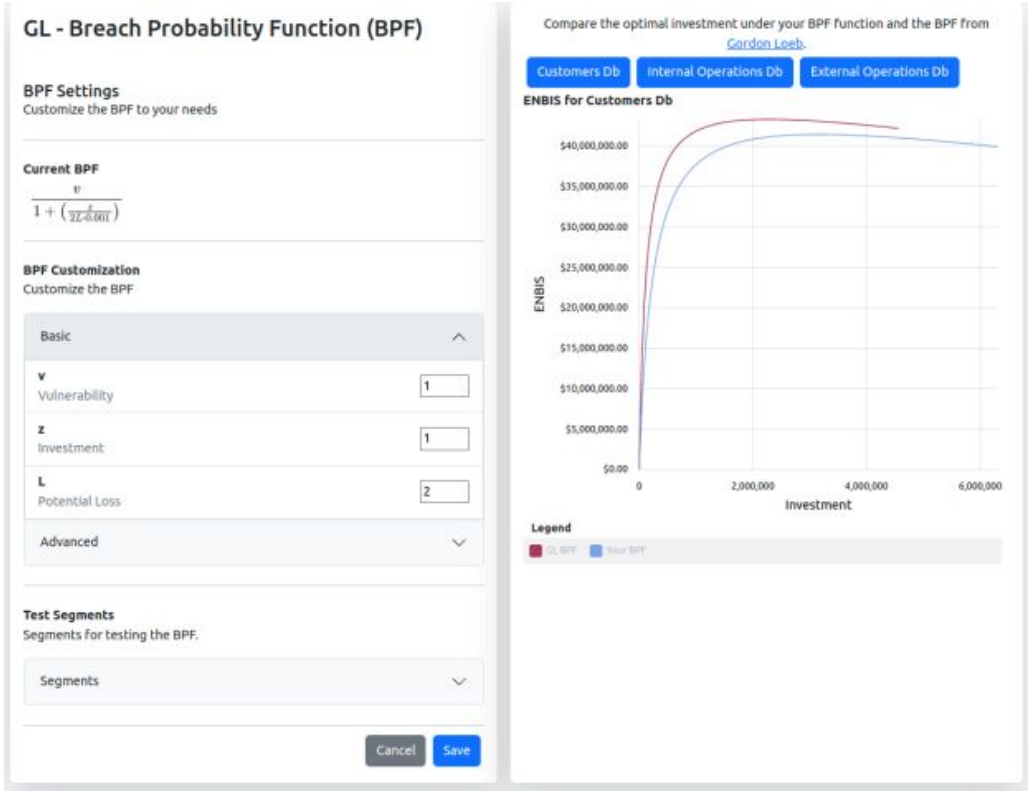
	Customers	Marketplace	Internal Operations	Total	Without Segmentation	Economic Benefits of Information Segmentation
Value of Information	500'000	6'000'000	3'000'000	9'500'000	9'500'000	
Calculated Vulnerability	12%	21%	3%		15%	
Expected Loss Before Additional Investments	60'000	1'260'000	90'000	1'425'000	1'425'000	
Optimal Investment	4'977	80'948	13'432	99'357	106'851	7'494
Expected Loss with Optimal Investment	5'477	86'949	16'431	108'857	116'351	7'494
Total Cybersecurity Costs	10'454	167'897	29'863	208'214	223'202	14'988

SECAdvisor - GL Calibration



Investment Analysis - Marketplace

Investment	Breach Probability	EBIS	ENBIS Rate
25000	0.041	1'016'129.032	991'129.032
0	0.21	0	0
10'000	0.079	787'500	777'500
20'000	0.048	969'230.769	949'230.769
30'000	0.035	1'050'000	1'020'000
40'000	0.027	1'095'652.174	1'055'652.174
50'000	0.023	1'125'000	1'075'000
60'000	0.019	1'145'454.545	1'085'454.545
70'000	0.017	1'160'526.316	1'090'526.316
80'000	0.015	1'172'093.023	1'092'093.023
80'948	0.014	1'173'051.479	1'092'103.479
90'000	0.013	1'181'250	1'091'250
100'000	0.012	1'188'679.245	1'088'679.245
110'000	0.011	1'194'827.586	1'084'827.586
120'000	0.01	1'200'000	1'080'000
130'000	0.009	1'204'411.765	1'074'411.765
140'000	0.009	1'208'219.178	1'068'219.178
150'000	0.008	1'211'538.462	1'061'538.462
160'000	0.008	1'214'457.831	1'054'457.831



GL - Breach Probability Function (BPF)

BPF Settings
Customize the BPF to your needs

Current BPF

$$\frac{v}{1+\left(\frac{z}{2L\cdot 0.001}\right)}$$

BPF Customization
Customize the BPF

Basic

v
Vulnerability
1

z
Investment
1

L
Potential Loss
2

Advanced

Test Segments
Segments for testing the BPF.

Segments

Cancel Save

Compare the optimal investment under your BPF function and the BPF from Gordon Loeb.

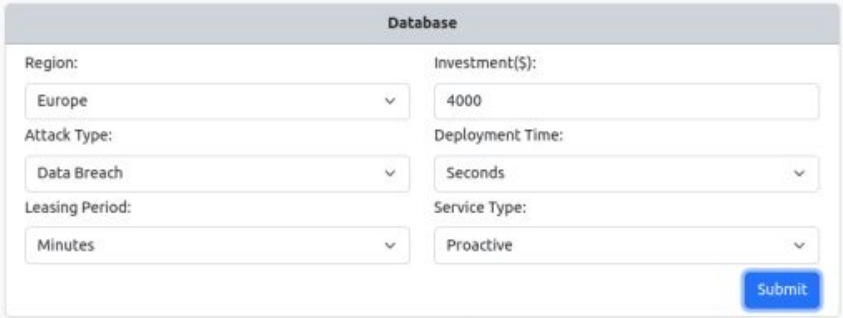
Customers Db | Internal Operations Db | External Operations Db

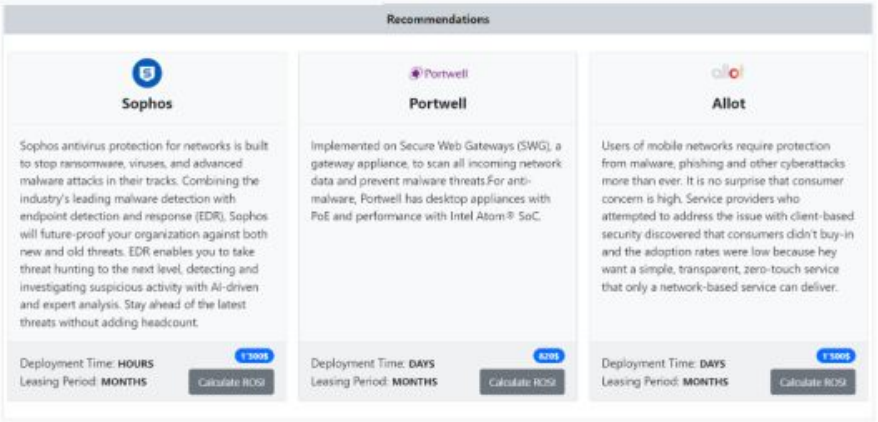
ENBIS for Customers Db

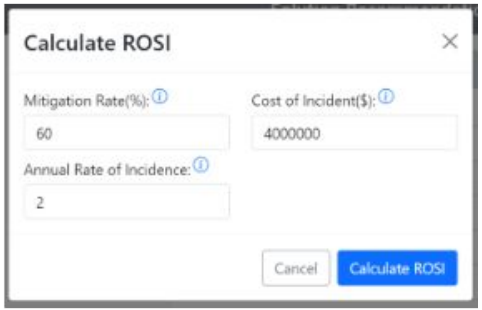
Legend

GL BPF | Your BPF

SECAdvisor - Recommendation







M. Franco, B. Rodrigues, B. Stiller: MENTOR: The Design and Evaluation of a Protection Services Recommender System; 15th International Conference on Network and Service Management (CNSM 2019), Halifax, Canada, October 21-25.

Usability Evaluation

- 13 participants, 6 tasks performed
  - Segments configuration, check the application of cybersecurity economics concepts intuitively and user-friendly
  - System Usability Score (SUS) equal to 82.1, which represents a very good usability

Task	Question	Answer	Success Rate
1	What is the vulnerability of the Database?	8%	92%
2	What is the yearly expected loss of the Database if there are no additional investments in cybersecurity?	$ 24,576	100%
3	After adding all the segments in the tool, how much is the economic benefits between the investment using information segmentation and without information segmentation considering the optimal investment?	$ 1,852	77%
4	How much is the total costs of cybersecurity for all of the segments?	$ 41,079	92%
5	Which recommendation provides the highest ROSI for the Network segment?	Portwell	92%
6	What is the optimal investment for the Database segment after adjusting for 1.5 the weight of the vulnerability (v) on the BPF?	$ 3,058	69.2%

Real-World Practical Activities

- First four editions (2020-2022) of the CONCORDIA Course "Becoming a Cybersecurity Consultant"
  - Around 120 participants used SECAdvisor during live webinars
  - Calculation of optimal investments, identification of protections, and selection of cost-effective protections
- Exercises as part of a cybersecurity lecture at UZH
  - Concepts of cybersecurity economics in practice for students
- Activities with 30 participants at the European Network for Cybersecurity (NeCS) PhD School 2023

Final Remarks

- Cybersecurity economic models are key for planning and cost management
  - SECAdvisor provides a low entry barrier to apply cybersecurity economic concepts in cybersecurity planning
- Quality of risk assessment and data are critical for economic analysis
  - Characteristics and behaviors vary, e.g., sectors and countries
- Calibration of economic models is still a complex task
  - There is no one-size-fits-all approach (yet)

Future Work

- SECAdvisor as a pillar for GT-IMPACTO, project being developed as part of the Hackers do Bem
  - Simulations and real-world statistics for applications of economic models
    https://inf.ufrgs.br/gt-impacto
- Automated data gathering to improve accuracy of economic models
  - Data from business, infrastructure, and protection systems
- Collaborative approach for data sharing
  - Business with similar characteristics and sectors

Obrigado!

Perguntas?

mffranco@inf.ufrgs.br

Estádio Beira-Rio, Porto Alegre, Brazil

Old Town, Zurich, Switzerland