

SECAdvisor: A Tool for Cybersecurity Planning using Economic Models

<u>Muriel F. Franco¹², Christian Omlin², Oliver Kamer², Eder J. Scheid¹², Lisandro Z. Granville¹, Burkhard Stiller²</u>

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



JFRGS

DE INFORMÁTICA

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)



"Risk comes from not knowing what you're doing." - Warren Buttet



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





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 Cost of





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

SECADVISOR			
ි Home	Actions		
🗐 🛛 Business Profile	Add new segment	0	Value of Informa
Segments	Show segment details	0	Calculated Vulne
Recommendation			Expected Loss Be Investments
③ Settings			Optimal Investm
Add segment	×	٦	Expected Loss w Investment
Add segment	×		Expected Loss w Investment Total Cybersecur
Add segment	Segment Type:		Expected Loss w Investment Total Cybersecur
Add segment Segment Name: Customers	Segment Type: Database ~		Expected Loss w Investment Total Cybersecur
Add segment Segment Name: Customers Enable value estimation:	Segment Type: Database ~		Expected Loss w Investment Total Cybersecu
Add segment Segment Name: Customers Enable value estimation: Value (\$): ①	Segment Type: Database ~ No O Yes Risk (%): 0		Expected Loss w Investment Total Cybersecur

Save

Segurite Station								
	Customers	Marketplace	Internal Operations	Total	Without Segmentation	Economic Benefits of Information Segmentation		
alue of Information	500'000	6'000'000	3'000'000	9'500'000	9'500'000			
alculated Vulnerability	12%	21%	3%		15%			
expected Loss Before Additional nvestments	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		
xpected Loss with Optimal nvestment	5'477	86'949	16'431	108'857	116'351	7'494		
otal Cybersecurity Costs	10'454	167'897	29'863	208'214	223'202	14'988		

Segments Overview



Success Rate (%):

20

SECAdvisor - GL Calibration

RPF Settings

×

Investment Analysis - Marketplace

Investment	Breach Probability	EBIS	ENBIS Rate
25000 0	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	1173'051.479	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)

Current BPF	
$\overline{1 + \left(\frac{t}{2L \cdot 0.001}\right)}$	
3PF Customization	
Customize the BPF	
Basic	^
v	1
Vulnerability	
z	1
Investment	
L	2
Potential Loss	
Advanced	~
Test Segments	
Segments for testing the BPF.	
Segments	~
	Cancel Save

Helis For Cust 540,000,000 533,000,000 530,000,000 525,000,000 515,000,000 515,000,000 55,000,000 55,000,000 55,000,000 55,000,000 50	000 000 000 000 000 000 000 000 000 00				
\$40,000,000 \$35,000,000 \$25,000,000 \$25,000,000 \$10,000,000 \$10,000,000 \$5,000,000	00 00 00 00 00 00 00				
\$35,000,000 \$30,000,000 \$25,000,000 \$220,000,000 \$15,000,000 \$15,000,000 \$55,000,000 \$55,000,000	00				
\$30,000,000 \$25,000,000 \$20,000,000 \$15,000,000 \$10,000,000 \$10,000,000 \$5,000,000 \$5,000,000 \$5,000,000	00				
\$25,000,000 \$20,000,000 \$15,000,000 \$10,000,000 \$5,000,000 \$5,000,000	00 00 00 00 00 00 00 00 00 00 00 00 00				
5 520,000,000 \$15,000,000 \$10,000,000 \$5,000,000 \$9	00				
\$15,000,000 \$10,000,000 \$5,000,000 \$5	00				
\$10,000,000 \$5,000,000 \$9	00				
\$5,000,000 \$0	00				
50					
	00		(
egend	0	2,000,000 Ir	4,00 westment	0,000	6,000,00
GLOFF	or DPP				

10

SECAdvisor - Recommendation

Recommendations

Region:		Investment(\$):	
Europe	~	4000	
Attack Type:		Deployment Time:	
Data Breach	~	Seconds	~
Leasing Period:		Service Type:	
Minutes	~	Proactive	~

Ξ 00 @Portwell Sophos Portwell Allot Calculate ROSI Users of mobile networks require protection Sophos antivirus protection for networks is built Implemented on Secure Web Gateways (SWG), a to stop ransomware, viruses, and advanced gateway appliance, to scan all incoming network from malware, phishing and other cyberattacks Mitigation Rate(%); Cost of Incident(\$): malware attacks in their tracks. Combining the data and prevent malware threats.For antimore than ever. It is no surprise that consumer industry's leading malware detection with malware, Portwell has desktop appliances with concern is high. Service providers who 60 4000000 endpoint detection and response (EDR), Sophos PoE and performance with Intel Atom® SoC. attempted to address the issue with client-based will future-proof your organization against both security discovered that consumers didn't buy-in Annual Rate of Incidence: new and old threats. EDR enables you to take and the adoption rates were low because hey threat hunting to the next level, detecting and want a simple, transparent, zero-touch service 2 investigating suspicious activity with Al-driven that only a network-based service can deliver. and expert analysis. Stay ahead of the latest threats without adding headcount. Cancel 8205 115005 Deployment Time: DAVS Deployment Time: DAYS Deployment Time: HOURS Leasing Period MONTHS Leasing Period: MONTHS Leasing Period: MONTHS

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.

×

Calculate ROSI

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	\$ 24 576	100%	
2	if there are no additional investments in cybersecurity?	\$ 24,370	10070	
	After adding all the segments in the tool,			
2	how much is the economic benefits between the	\$ 1 852	770%	
5	investment using information segmentation and without	\$ 1,032	1170	
~	information segmentation considering the optimal investment?			
1	How much is the total costs of cybersecurity	\$ 41 070	02%	
4	for all of the segments?	\$41,079	9270	
5	Which recommendation provides the highest ROSI	Dortwall	02%	
5	for the Network segment?	TORWCII	9270	
	What is the optimal investment for the Database segment			
6	after adjusting for 1.5 the weight of the vulnerability (v)	\$ 3,058	69.2%	
	on the BPF?			



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