Understanding your Return on Security Investment (ROSI)

(Or: How I survived as a security guy working for the CFO)

James Callahan

Objective

- Understand basics of Security ROI (ROSI)
- Provide high level overview of each subcategory.
- Understand some of nuances of Security Value Add as a factor of ROSI.

- The world according to Callahan.
  - Don’t have all the answers.

Rules of Thumb

Calculating ROSI is a small part of a big process.

There is no silver bullet…

Crime = Motive x Opportunity
Do your own Business Impact Analysis

Security is both an Art and a Science

Precision vs. Accuracy!

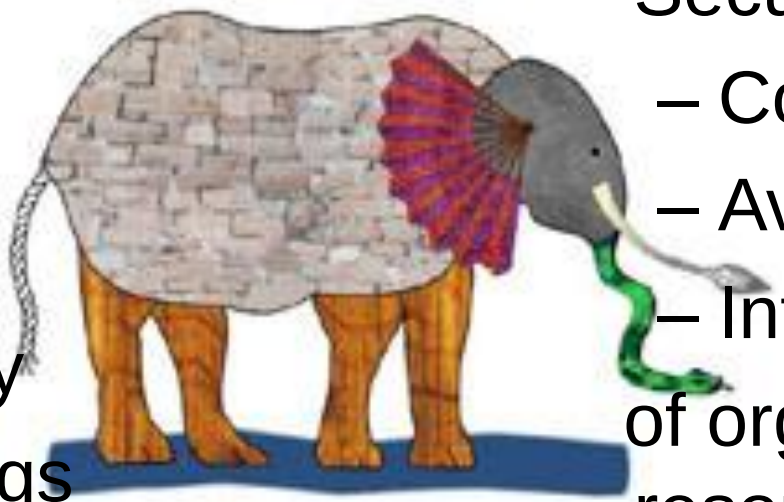
In ROSI it is better to be accurate than precise. The 80/20 rule.

ROSI Pitfalls

Just when you think you know how to measure it, there is something else to consider.

High Level Definitions

- ROI Objective
  - Revenue generation
  - Increased productivity
  - Cost savings



- Security Objective
  - Confidentiality
  - Availability
  - Integrity

of organization resources

Bringing these together is like mating elephants. It's done on a very high level. There's a lot of stomping and screaming involved. And it takes years to get any results. -www.jokes2go.com

ROSI comes in several flavors

- Decreased Risk
  - Loss Reduction
  - Cost Reduction
- Increased Efficiency
  - Getting things done quickly
  - Efficient applications of mandated requirements.
- Security Value Add
  - Employee Contentment
  - Regulatory Compliance
  - Customer Satisfaction

ROSI

- Decreased Risk
  - Loss Reduction
  - Cost Reduction
- Increased Efficiency
  - Getting things done quickly
  - Efficient applications of mandated requirements.
- Security Value Add
  - Employee Contentment
  - Regulatory Compliance
  - Customer Satisfaction

Decrease Risk

- To measure risk it must be defined:
  - Risk is a probable event with adverse consequences.
  - Security Risks are categorized as **Threats or Vulnerabilities**.

- Then risks need to be measured – Risk Analysis
  - **Quantitative** – attempts to assign real numbers to the costs of safeguards and the amount of damage that can take place.
  - **Qualitative** – An analysis that judges an organization's tolerance to risk. This is largely based on judgment, intuition, and the experience, vice mathematics.

Quantitative Decreased Risk ROSI

- Many different formulas.
- Many more supporting metrics.
- Even more ways of calculating those metrics.

Bottom line:

- Quantitative ROSI formula is a product of the type of risk mitigation the security countermeasure brings.
  - Reduced Threat (or exposure) OR
  - Reduced Vulnerability (or rate of occurrence)

Remember Rule of Thumb: Precision vs. Accuracy!

In ROSI it is better to be accurate than precise. The 80/20 rule.

Calculating Decreased Risk ROSI

based on **Quantitative** Risk Analysis

Some Definitions

- Exposure Factor (**EF**) = Percentage of asset loss caused by identified threat; (0 to 100%) (*This threat will cause x% degradation of asset value*)

- Single Loss Expectancy (**SLE**) = Asset Value x Exposure factor; 1,000,000 @ 10% EF = $100,000.

- Annualized Rate of Occurrence (**ARO**) = Estimated frequency a threat will occur annually or fraction thereof.

- Annualized Loss Expectancy (**ALE**) = Single Loss Expectancy x Annualized Rate of Occurrence.

- Safeguard cost/benefit analysis **(SCB) =** (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard or **ROSI.**

Reduced ARO

- Straight Forward
  Safeguard cost/benefit analysis = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard).

  This formula assumes 100% reduction in ARO.

- Reduce ARO by a percentage.
  Multi-Safeguards Possible (here x & y)
  Safeguard cost/benefit analysis =
  ARO X Safeguard (x) Effectiveness = Modified ARO x
  ARO X Safeguard (y) Effectiveness = Modified ARO y
  SLE X Modified ARO (y or x) = mALE (y or x)
  ALE – mALE (y or x) = Savings (y or x)
  Savings x – Safeguard x cost = ROSI for y
  Savings y – Safeguard y cost = ROSI for x

Sample Spreadsheet

Asset Value (AV)	200000	Replacement / Recovery / Reporting /			
Exposure Factor (EF)	75.00%	Percentage of asset loss caused by identified threat (Single Event)			
Single Loss Expectancy (SLE)	150000	AV x EF			
Annualized Rate of Occurance (ARO)	2	Estimated frequency a threat will occur (or fraction thereof)..			
Annualized Loss Expectancy (ALE)	300000	SLE x ARO			
Safeguard 1 cost (Decreased Threat)	5000	Safeguard 1 Effectiveness	75.00%	Annualized percent reduction in ARO	
Safeguard 2 cost (Decreased Threat)	60654	Safeguard 2 Effectiveness	33.00%		
Safeguard 3 cost (Decreased Threat)	6521	Safeguard 3 Effectiveness	80.00%		
Safeguard 4 cost **(Reduced EF)**	30000	Safeguard 4 Effectiveness	20.00%	**Percent reduction in EF**	
ARO	**X**	**Safeguard Effectiveness**	**=**	**Modified ARO**	
2		0.75	1.5	mARO 1	(for Safeguard 1)
2		0.33	0.66	mARO 2	(for Safeguard 2)
2		0.8	1.6	mARO 3	(for Safeguard 3)
EF	**X**	**Safeguard Effectiveness**	**=**	**Modified EF**	
75.00%		0.2	15.00%	mEF 4	
SLE	**X**	**mARO**	**=**	**mALE**	
150000		1.5	225000	mALE1	
150000		0.66	99000	mALE2	
150000		1.6	240000	mALE3	
ALE	**-**	**mALE**	**=**	**Savings**	
300000		225000	75000	Savings for safeguard 1	
300000		99000	201000	Savings for safeguard 2	
300000		240000	60000	Savings for safeguard 3	
Savings	**-**	**Cost**	**= ROSI**		
75000		5000	70000	Safeguard #1	
201000		60654	140346	Safeguard #2	
60000		6521	53479	Safeguard #3	

Sample Spreadsheet

EF	**X**	**Safeguard Effectiveness**	**=**	**Modified EF**		
75.00%		20.00%	15.00%	mEF 4		
Asset Value (AV)	200000	Replacement / Recovery / Reporting /				
m Exposure Factor (EF)	15.00%	Percentage of asset loss caused by identified threat (Single Event)				
mEF Single Loss Expectancy (SLE)	30000	AV x mEF				
mEF Annualized Loss Expectancy (ALE)	60000	mEF SLE x ARO				
Safeguard 1 cost (Annualized)	5000	Safeguard 1 Effectiveness	75.00%	Percent reduction in ARO		
Safeguard 2 cost	60654	Safeguard 2 Effectiveness	33.00%			
Safeguard 3 cost	6521	Safeguard 3 Effectiveness	80.00%			
ARO	**X**	**Safeguard Effectiveness**	**=**	**Modified ARO**		
2		0.75	1.5	mARO 1		
2		0.33	0.66	mARO 2		
2		0.8	1.6	mARO 3		
mEF SLE	**X**	**mARO**	**=**	**mEFmALE**		
30000		1.5	45000	mEFmALE1		
30000		0.66	19800	mEFmALE2		
30000		1.6	48000	mEFmALE3		
mEF ALE	**-**	**mALE**	**=**	**mEF Savings**		
60000		45000	15000	Savings for Safeguard #1 + #4		
60000		19800	40200	Savings for Safeguard #2 + #4		
60000		48000	12000	Savings for Safeguard #3 + #4		
mEF Savings	**-**	**Cost**	**= ROSI**			
15000		35000	10000	Safeguard #1 + #4		
40200		90654	-20454	Safeguard #2 + #4		
12000		36521	5479	Safeguard #3 + #4		

Risk : Individual Laptop Theft – 500 Deployed Laptops	**Without Safeguard**	**With Safeguard**
Asset Value ($3500 each Replace + TCL + Recovery)	$6000	$6000
Exposure Factor (**EF**)	100%	20%
Single Loss Expectancy (**SLE**) (AV x EF)	6000	1200
Annual Rate of Occurrence (**ARO**) (Frequency event could occur) (3%)	15	15
Annual Loss Expectancy (**ALE**) (SLE x ARO)	90000	18000
Safeguard Costs		
Hardware ($35 Laptop Cable * 500)	+ $17500	
Software ($20 Tracing Software Program * 500)	+ $10000	
Deployment Costs (% of annual salary dedicated to deploy & maintain) (50,000 p/y 3% of time spent administering program)	+ $1500	
Safeguard Annual Cost (**SAC**)	$29000	
Annual Safeguard Cost Benefit: (**SCB**) (ALE w/o – ALE w)	$72000	
Projected Savings (SCB – SAC)	$43000	
Risk Response (Negative Number = Accept/ Positive Number = Mitigate)	Mitigate	

Simple Quantitative Sample

Reduced EF as stand alone safeguard

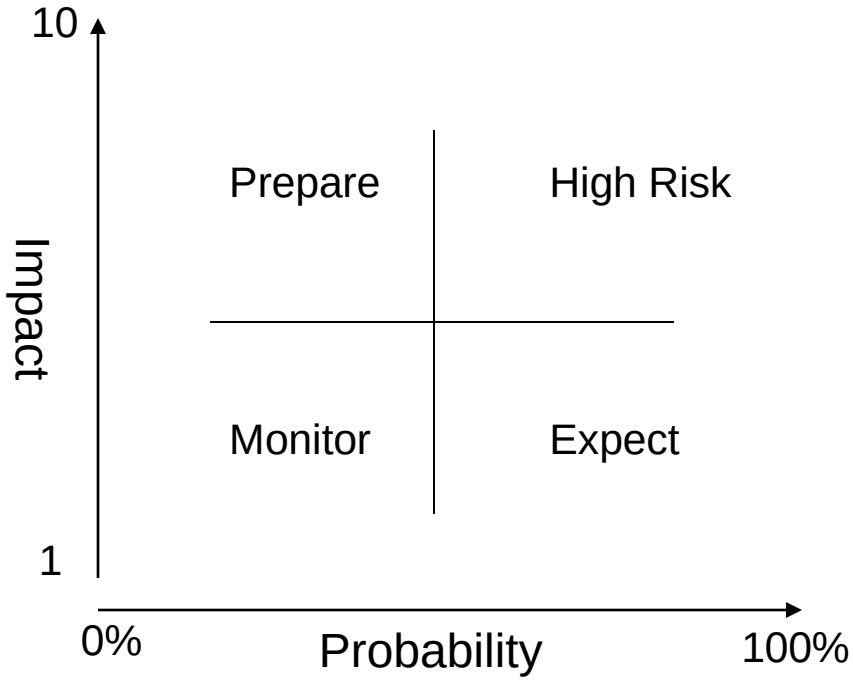
Risk : Unauthorized Destructive Access to Corporate Internal Servers.	**Amount**
Asset Value – R&D Server Data	$200,000
Exposure Factor (**EF**) (75% of data also in other locations)	25%
Single Loss Expectancy (**SLE**) (AV x EF)	50000
Annual Rate of Occurrence (**ARO**) (Frequency event could occur)	.1
Annual Loss Expectancy (**ALE**) (SLE x ARO)	5000
Safeguard Costs	
Hardware ($x amortized over y years) (Firewall $2000 / 5)	+ $400
Software ($x amortized over y years) ($1100 + training/Maintenance and Renewal)	+ $400
Support personnel (each year) (% of annual salary) (50,000 * 10%)	+ $5000
Safeguard Annual Cost (**SAC**)	$5800
Annual Safeguard Cost Benefit: (**SCB**) ALE – SAC 5000-5800	-$800
Project Savings ALE - SCB	$5800
Risk Response (Negative Number = Accept/ Positive Number = Mitigate)	Mitigate

Simple Quantitative Sample

Qualitative Risk Analysis Methods

- Delphi Technique
  http://www.cce.cornell.edu/admin/program/documents/delphi.htm
- Brainstorming
- Surveys
- Questionnaires
- Check Lists
- Interviews
- Charting

Qualitative Risk Analysis

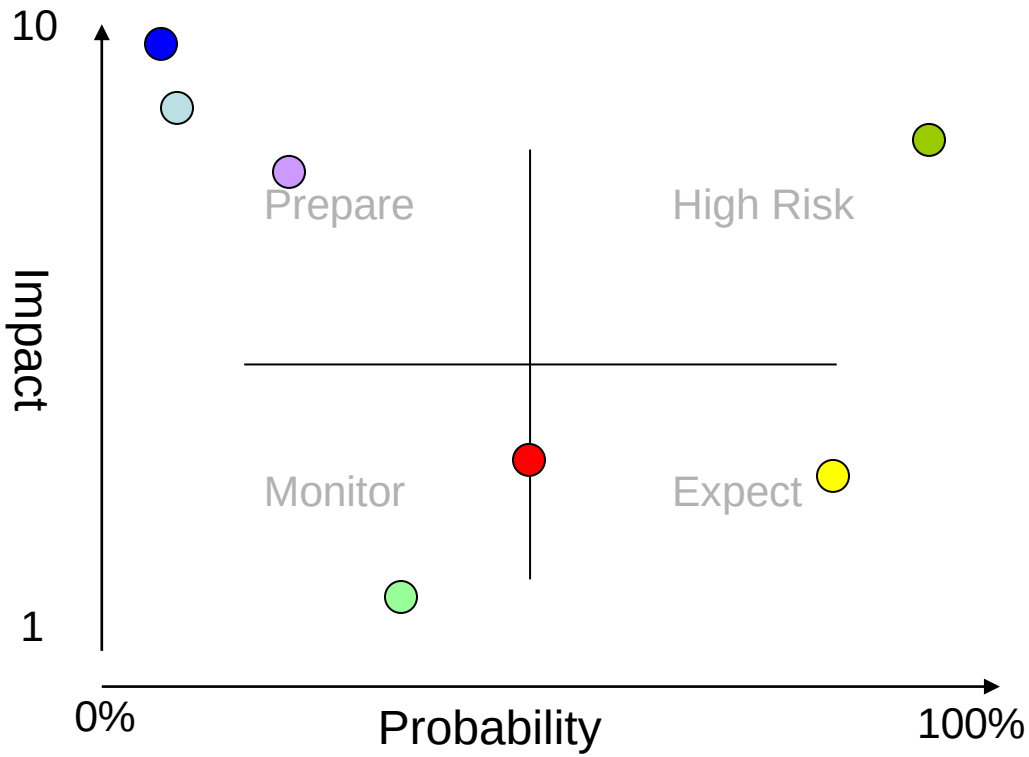


- Simple and easy to prepare.
- No cost benefit analysis.
- Subjective in metrics and risk assignment.
- Completed with Interviews or surveys.

Best (quickest) for prioritizing spending of fixed budget

Qualitative Risk Analysis

Sample



Risk	P	I
Tornado	15	9
IT Virus	99	8
Civil Unrest	50	3
Hard drive Failure	80	3
Database Corruption by hackers	1	10
Work Place Violence	20	7
Petty Theft	33	2

ROSI

- Decreased Risk
  - Loss Reduction
  - Cost Reduction
- Increased Efficiency
  - Getting things done quickly
  - Efficient applications of mandated requirements.
- Security Value Add
  - Employee Contentment
  - Regulatory Compliance
  - Customer Satisfaction

Increased Efficiency

Sometimes, security can be overly bureaucratic …

- Looking for bottlenecks, hurdles or hoops.
  - Single Sign On Technology
  - Entrance Doors
- Selecting Access Control System based on usability.
- Increase security device throughput.
- Automate processes (do you really need a physical signature?)

Systems vs. Process based security models.

Calculating Increased Efficiency

- Calculate Total Cost of Ownership both with and without improvement.
- TCO
  - Procurement
  - Maintenance
  - Operations
  - Training
  - % of payroll

What are your costs without the improvement vs. with the improvement
Time / Facilities / Utilities / Other Operating

ROSI

- Decreased Risk
  - Loss Reduction
  - Cost Reduction
- Increased Efficiency
  - Getting things done quickly
  - Efficient applications of mandated requirements.
- Security Value Add
  - Employee Contentment
  - Regulatory Compliance
  - Customer Satisfaction

Security Value Add
Employee Contentment

- Security needs to be visible and proactive.
- Plans need to be communicated and rehearsed.
- Employees need to be energized towards the security objectives.
- Must be balanced to mitigate vice create FUD (fear uncertainty doubt)
- How to measure
  - Employee Surveys
  - Employee Retention
  - Exit Interviews
  - Number of calls to Security

Security Value Add
Regulatory Compliance

- HIPPA / GLB / Safe Harbor
- Privacy and Security are often intertwined.
- Government Regulations are a moving target.

Insurance Issues

- Work with carrier to determine if there is an insurance cost benefit to upgrading or maintaining high security.

Security Value Add

Buying from Secure Vendors

- Get your security team involved in this process.
- Audit service providers for compliance.
- Set minimum standards for safeguarding your resources.
- Your security is only as strong as that of your weakest supplier.
- Some regulations now mandate this (HIPPA, GLB, etc.)

Security Value Add
‘Selling Security’

- Relationships are built on trust. Security programs need to be center stage, helping to engender that trust in clients.
- Incorporate Security into product offering.
- Security needs to be integrated into corporate culture.

Ok, I’m sold – so how do I do this?

‘Selling Security’
So How?

- Solid Program of Policies; Procedures; Roles & Responsibilities.
- Include Security in marketing collateral and the sales cycle.
- Build a world class team with diverse composition.
- Staying on top of innovations and situations.

Summary

- Understand basics of Security ROI (ROSI)
- Provided high level overview of each subcategory.
- Understand some of nuances of Security Value Add as a factor of ROSI.

Understanding your Return on Security Investment (ROSI)

James Callahan