CERIAS

The Center for Education and Research in Information Assurance and Security

Investment in IT Security: Do we reap as much as we sow?

*Supported by Intel

By Swarnalakshmi Iyer

Background

Trends from the past five years show a consistent rise in the amount spent on IT Security. On the other hand, the losses from cyber breaches have also consistently risen. Do we get our money's worth with the investments in IT Security? The Return On Security Investment (ROSI) Model and the Gordon-Loeb Model provide a way to perform cost-benefit analysis for IT Security Investments. This research attempts to validate these models using figures from past data.

The Return on Security Investment (ROSI) Model

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

Example 1:

The Acme Corp. is considering investing in an anti-virus solution. Each year, Acme suffers 5 virus attacks (ARO=5). The CSO estimates that each attacks cost approximately 15.000 € in loss of data and productivity (SLE=15.000). The anti-virus solution is expected to block 80% of the attacks (Mitigation ratio=80%) and costs 25.000€ per year (License fees 15.000€ + 10.000€ for trainings, installation, maintenance etc.).

The Return on security investment for this solution is then calculated as follow:

$$ROSI = \frac{(5 * 15000) * 0.8 - 25000}{25000} = 140\%$$

According to this ROSI calculation, this anti-virus solution is a cost-effective solution.

*Source: ENISA- Introduction to Return on Security Investment

The Gordon-Loeb Model Result

Every additional dollar spent on security does not necessarily add as much value as the previous dollar spent. Firms should invest ≤ 37% of Expected Loss

1. Estimate potential loss (L) from security breach for each set of information. The inverse of this becomes the value of the information (high, medium and low)
2. Estimate the likelihood that an information set will be breached by examining its vulnerability/threat (v) to attack
3. Create a grid with all the possible combinations of the first two steps, from low value (low L, low v) to high value (high L, high v)
4. Focus on spending where it should reap the largest net benefits based on productivity of investments

			Value of Information Set = Potential Loss (L)		
			Low	Med	High
			$10M	$50M	$90M
Vuln/Threat (v)	Low	10%	$1M	$5M	$9M
	Med	50%	$5M	$25M	$45M
	High	90%	$9M	$45M	$81M

Table 4 - Potential Loss (L) based on information set value and vulnerability/threat (v)

From Table 4 the average potential loss (L) from a medium vulnerability/threat (v) against a medium value information set is $25M. Based on the Gordon-Loeb Model, we should spend on average no more than $9.25M (37% of $25M) to protect this information. Please note that the above table is a summary of much more detailed work done by Gordon and Loeb.

*Source: http://cybervelocity.com/cybersecurity-economics-for-cio-and-ciso/

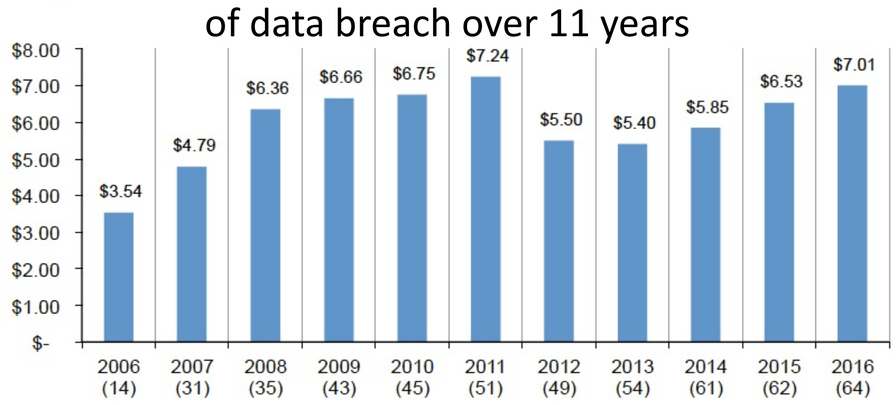
Median Budget and Percentage Allocated to Security by Year by Industry

Industry	IT Budget FY 2014	IT Budget FY 2015	IT Budget FY 2016 (Projected)
Financial services	$1M	$500K–$1M	$500K–$1M
Technology/IT services	$100K	$100K–$500K	$100K–$500K
Government	$500K–$1M	$500K–$1M	$1M–$10M
Education	$1M–$10M	$1M–$10M	$1M–$10M
Health care	$1M–$10M	$1M–$10M	$1M–$10M

Industry	% Budget for Security FY 2014	% Budget for Security FY 2015	% Budget for Security FY 2016 (Projected)
Financial services	7%–9%	7%–9%	10–12%
Technology/IT services	1%–3%	4%–6%	4%–6%
Government	4%–6%	4%–6%	7%–9%
Education	1%–3%	3%–4%	1%–3%
Health care	4%–6%	4%–6%	4%–6%

*Source: Sans IT Security Spending Trends

The average total organizational cost of data breach over 11 years



*Source: Ponemon - 2016 Cost of Data Breach Study: United States

Research Objective

To test the models against past data to answer the following questions:

- Is optimal cyber security spending quantifiable?
- If yes, How to quantify optimal spending?

Research Methodology

This research attempts to assess the returns on IT Security spending at a pan industry level. Data available on average investment in IT Security spending as well as data on average cost of cyber breach for organizations in X industry is fed into each of the models. The results are to be evaluated to see if the models show an over spending or underspending or optimal spending. Data for the top five industries from the past five years will be used for this study.

CERIAS

PURDUE UNIVERSITY