Abstract

Many organizations are looking at investing in cybersecurity and this document will provide some of the current thinking and methods around return on cybersecurity investment. While each organization has different needs, every investment including cybersecurity investments must be reviewed to determine if it provides an adequate return or the organization will not be successful.
Research Question

This paper is designed to look at the question of how to measure return on investment for cybersecurity. The threat of cyber-attacks is growing and the potential damage from these attacks is greater than ever. With that understanding, all organizations are deciding how to protect themselves against attacks within their operating budget. As organizations make decisions about what to spend on security, there is a lack of effective measurement to determine which investment is generating what return and this information is crucial in making future spending decisions. While every organization will have a different cost benefit analysis and business need, this paper will provide information and guidance to any organization looking to make better security investment decisions.

The report is organized in the following manner

Section 2: Introduction
Section 3: ROI and Corporate Finance
Section 4: Literature Review
Section 5: Potential Approaches
Section 6: Final Remarks
Introduction

Organizational leaders today are being asked to maximize shareholder value or achieve the mission of the organization while being attacked through some of their most critical systems and assets. These attacks can be basic attacks that are easily understood, or are extremely complex and have never been seen before. For many organizations, cyber risks are growing very quickly and the potential damage of these attacks is growing as well. This increase in potential damage should result in additional spending or additional risk management requirement but with the advances in technology and different opinions on how best to deal with the problem, an organization has many choices on where to spend security dollars. When considering this security spending, an organization must determine where their risk tolerance is, where their priorities are, and how to determine what is the right level of investment while getting the most return for their security resources. As companies continue to budget and forecast looking ahead, the issue of how much to spend and the return on that spending is one that must be determined.

While some programs are able to more easily justify funding levels based on the type of service they provide, security programs have a fundamental challenge of not bringing in any additional revenue. As traditional ROI models measure the increased revenue that is created by the investment in comparison with the additional cost, this does not work for security programs. But instead of focusing on revenue, organizations can focus on loss prevention and this loss avoidance can be measured and estimated and used in a statistical analysis.
ROI and Corporate Finance

In order to discuss return on investment for cybersecurity, and the economics of cybersecurity in general, it is important to have an understanding of the terminology of ROI and the basic theory of it in corporate finance. This is important because while ROI is a simple concept, it is more valuable for an organization when considered through the lens of corporate finance. Throughout the rest of this section, we will discuss ROI in terms of profit and loss and return which may not be applicable for certain organizations, government etc, but can be tailored to those cases as well.

Return on investment is a basic concept that describes what an organization or person will receive after making a particular investment. These returns can be in dollars if the investment is in a financial instrument such as a stock, or in improved business process that will generate additional dollars such as a factory. Recently there have been efforts to try and determine return on investments that do not provide additional dollars in return or improve the ability to generate additional revenue. Initiatives such as training, security, and other non-revenue generating programs often require significant investment but organizations have had very little way to quantify the returns they receive. While there are no perfect measurements that have been determined yet, there has been progress, and this progress gives ROI much more use as a benefit of ROI is that it is a common way to measure and compare potential investments against each other. At a basic level, if one investment has a higher return than another, the first investment is more likely to be made.

According to Modigliani and Miller\(^1\) in their 1958 article in the American Economic Review, the acquisition of an asset is justified if it increases net profit, or adds more to the market value of the firm than the acquisition cost. These criteria seem very simple, but are made slightly more complex when the idea of the cost of capital is brought up. For the asset to truly increase net profit, the rate of return must be greater than that of the rate of interest. Another way to look at this is, the investment should be made only if it is better than the opportunity cost of the purchase price. When considering investments in cybersecurity, the exact numbers may be harder to determine, but the theory is the same.

If a company is considering an investment to improve their cybersecurity, it is likely they have

other potential need areas where that money could be spent and the organization could always put the money in the bank and receive interest. In corporate finance, this rate of interest is usually estimated to the return on the 10 year bond, so any investment in cybersecurity should be able to return more than the current return on a ten year bond or the investment should not be made. Also the required rate of return for an investment may depend on how the funds for the investment was raised (operations, debt, etc.) which is beyond the scope of this section but for example if capital had to be borrowed as it is a major cybersecurity investment, then the rate of borrowing would impact the required rate of return on the cybersecurity project.

For organizations considering an investment in a plant or other physical asset, this theory offers a way to look at their investment decisions as they can estimate the added revenue brought in by the potential investment over its lifetime and determine if it is better than alternative investments and the rate of interest. Unfortunately for cybersecurity, there is no great way to determine the return or quantify the results of a cybersecurity project which makes this task much more challenging. The following section will go into some of the leading ideas around quantifying cybersecurity and these methods may be able to provide numbers that could be weighed against the cost of capital to determine appropriate investment. This idea is important to understand for decision makers and cybersecurity program managers as they try and budget accurately and defend investment decisions. It may not be enough to persuade an Executive with a possible return unless that return can be compared with other potential uses for that budgeted funding.
Literature Review

In my research there did not appear to be a standardized method for the measurement of ROI, but there have been articles and papers written that look at the subject from an academic, technical, and business perspective. For this paper the focus was on documents from each of these perspectives and how each of them can contribute to a better way to review and potentially measure security investments.

1. European Network and Information Security Agency (ENISA) – Introduction to the Return on Security Investment

This document focused on the justification of CERTs in organizations and introduced a metric, Return on Security Investment (ROSI). It identified the same issue as was discussed in the introduction, that security is not a revenue producing investment, but prevents loss. To provide any quantitative measure, the focus must be on how much loss was prevented versus the amount that was spent to prevent it.

To achieve the quantitative measurement that many organizations are looking for, ENISA recommends starting with the components of risk. The risk components specifically called out are:

- Single Loss Expectancy (SLE) = the total amount of loss for one occurrence
- Annual Rate of Occurrence (ARO) = the probability that a risk will happen in a year
- Annual Loss Expectancy (ALE) = SLE*ARO

By using these components of risk an organization is able to determine the ROSI which equals monetary loss reduction – cost of solution / the cost of solution. The monetary loss reduction is determined by the difference between ALE and the modified ALE after the security solution has been put in place

The limitations of this approach are similar to the limitations on all of the other approaches that were proposed in the documents. Many of the components of the return models are based on estimates which may not be accurate or actuarial data which may not have many years of history.
2. **Security ROI: Fact or Fiction – Bruce Schneier**

Mr. Schneier believes that ROI is not meant for security. Because security is not an investment that provides a return but an expense that hopefully pays for itself through loss prevention, the term ROI does not apply for security.

The classic method as mentioned in the ENISA article is the ALE formula. But as ENISA pointed out in their limitations, the data used for this is crucial to the value of the formula. The lack of good data about general cybersecurity trends and specific configuration of specific measures makes this very challenging. To make the challenge greater, the threat moves too quickly so when good data does become available usually the threat has changed and the data is no longer valuable.

Another issue with this model and way of thinking is when an organization is considering a rare and expensive event. Because the impact of a cyber-attack may result in huge damages, estimating the impact may result in huge number for security that is not reasonable.

In conclusion Mr. Schneier believes that ALE can be used as a general guideline but make sure the data that it is based on is as good as possible, and not influenced by the person performing the calculations, like a vendor.

3. **The economics of Security Investment – Gordon and Loeb, 2002**

While this is over ten years old now, it is the most referenced work in the documents that were reviewed and seems to set up a lot of the discussion since its publication. Due to the age of the document, many of the statistics were not as relevant but the model is still very important today. Also, this is not a math focused paper so many of the more complex math points will not be reviewed below.

Their model is based on a firm contemplating the provision of additional security to protect given information set. A particular information set is characterized by three parameters:

- Loss on a breach occurring
- The probability of the threat occurring
The vulnerability which is the probability that a threat once realized would be successful.

In their paper, the authors assume that this is a fixed amount estimated by the firm and they do not consider catastrophic losses in their work. For the threat parameter they assume that there is a single threat to an information set. In general, the model the authors create assumes that firms can change the vulnerability of information but cannot reduce the threat.

The authors believe that the Expected Benefits of an Investment in information Security (EBIS) is equal to the reduction in expected loss. EBIS minus the cost of the security is the Expected Net Benefits from an Investment in information Security (ENBIS).

Three main assumptions were used when developing the functions they worked with:

1. A1 – if initially the attack success probability is 0, it stays so after every possible investment
2. A2 – if no money is invested, there will be no change in attack probability
3. A3 – The function S is continuously twice differentiable

Through using their model with that data available, the authors determined that for two large security breach probability classes that represent a wide range of functions, the optimal investments in information security never exceeded 36.79% of the expected loss.

In summary their finding was that optimal expenditures do not always increase with the increase in vulnerability and expenditures on security should almost never exceed 37% of potential loss.


The author believes that some models have been created around measurement of security investments, but these methods are not integrated with financial analysis methods. This is important to consider as BASEL II requires risk to be an accountable measure which will increase the importance of measuring security risk.
BASEL II requires that operational risk is included in the calculation for necessary regulatory capital and because of this many models around risk management have been developed. The author states that the Loss Distribution Approach (LDA) is the best known approach used when considering risk management and regulatory capital calculation.

In terms of measuring performance of information security investments, the author states that risk mitigation is an appropriate method for measurement. Return on Security Investment would be improved if risk mitigation effects were calculated properly including the scenario analysis and expected values.

5. An Overview of the Economics of Cybersecurity and Cybersecurity Policy, Joseph Cordes, June 2011

The author presents the idea that there is a demand and supply model for cybersecurity. Because both attackers and defenders have to spend time and resources to attacking or defending there is a point where each of them will not spend additional time and resources. This sort of model and analysis can help determine how a range of factors affect the incentives for attacks and defense and can potentially help determine how things will change depending on cost and reward changes.

For defenders, the relevant incentives that impact the appropriate level of security is the economic payoff and the economic cost while attackers have economic or political payoff and the economic cost.

According to the authors, the chosen level of cybersecurity may not lead to a balance of social benefits and costs and there are three major cases where private investments in cybersecurity are less than the social benefits.

- Network externalities – In the case of cybersecurity, the benefits of early adoption may be less than the cost until a critical mass is developed.
- Information asymmetries and lemons problems – quality attributes of cybersecurity technology can be difficult to verify and vendors know more than the buyers. Because of this a higher quality but more expensive product may not survive
- Coordination failures – If two organizations are looking to improve cybersecurity, each organization may not invest hoping the other will make the investment
Because private markets cannot necessarily provide the socially appropriate level of security, policy options exist to make up the difference. There are low intervention methods such as removing barriers to information sharing and clarifying liability while more active methods such as regulation and investment in R&D also exist.
Potential Approaches

When an organization is trying to determine the value of their security investments, they have a number of options they can consider. As referenced in much of the literature on the subject, an organization can use a model focused on the Annual Loss Expectancy (ALE) concept. Finally an organization could look at a different approach than discussed in the literature which is an ROI approach based on Key Performance Indicators.

ALE Approach

Rather than summarize the ALE approach discussed in much of the existing literature and in the section above, there are additional inputs that should be considered by an organization depending on their sector, size, and other factors. The basic formula in the ALE method is the amount of loss for an event multiplied by the number of times it occurs per year. This makes sense and is a good way to consider an individual decision that only impacts one specific area or control. Unfortunately for cybersecurity, one investment almost always will fit into a larger set of controls or security and the impact of an investment in one part of the network or organization may be seen in a different part of the security system. With this in mind, there are a few other inputs that impact potential losses that organization should consider adding to the ALE model to improve the accuracy of the results.

Compliance with Regulation or Industry Requirements

While this does not apply to all organizations, many organizations are looking to improve their cybersecurity because of attacks on themselves or others in their industry or industry regulations that have been put in place. Usually the organization has a choice on how best to comply with these requirements but not complying with them can result in loss of business if they are a supplier to the government or even fines. These fines are potential losses that the organization must avoid and for example in the energy industry, the Federal Energy Regulatory Commission (FERC) has the legal ability to impose fines of up to a million dollars a day for some violations. Other regulators have a similar legal ability or can create other negative consequences for organizations. Depending on the organization, these potential fines or other negative consequences should be factored into the ALE equation. A potential metric could be Annualized Compliance Benefit (ACB)
and the equation would look like \( \text{SLE} \times \text{ARO} - \text{ACB} = \text{ALE} \). If compliance or regulation is not relevant to an organization they do not need to use it, but if attacks and damage becomes more of an issue, other regulators may look to enforce some standards and organizations will need to consider ACB.

**New Business from More Security Focused Customers**

One of the major areas of concern for a lot of organizations now is security around their supply chain. Even if the organization has great security, if the companies they work with do not then threats can still be successful. So if an organization decides to invest in additional cybersecurity, they may make themselves more attractive as a partner or supplier to other firms since they may bring fewer security concerns than their competition. Also, unlike most of the returns on cybersecurity, new business can be quantified with additional revenue and depending on the new business, a certain percentage should be attributed to the cybersecurity investment. In terms of the ALE equation, this return would not be included since it does not impact potential loss, but it should be included in the discussion after the ALE has been calculated.

**Reputation, Brand, and Goodwill**

As demonstrated by the recent attacks on Target and other retailers and the reaction to the attacks, it is not just lost sales that an organization has to manage. While it is hard to quantify the impact to their reputation and how many people will make different shopping decisions, it must be included in any calculation around security. The value of keeping the organization out of the media and their reputation and brand clean is a large driver of security by some types of organizations. One potential way to look at this potential loss of reputation and brand is to look at goodwill. It is included on organization balance sheets and protection of that goodwill or potential losses around that goodwill could be included in the ALE equation. Some organizations may consider this as part of the SLE but if they are looking at SLE more narrowly, then they should consider a Goodwill Loss Expectancy (GLE)

**Information Sharing**

If an organization has better security, other organizations will feel more comfortable sharing information. This information sharing can reduce potential losses from a cyber-attack even further.
than just the result of the investment as information on threats, trends, or the environment can be shared and used to improve the security of the organization. When organizations are making the cybersecurity investment, they may only be thinking of how that investment will impact their security in a specific way. But by improving their overall security and being trusted with additional information they may reduce their potential losses by even more than was expected. How much information is shared will change depending on the sector the organization is operating in and the overall maturity level of the sector as a whole. For some organizations, the ability to participate in information sharing or increase their level of sharing will have a significant impact on reducing threats and vulnerabilities and these firms must include this in their ALE equation. It can either be included as part of the SLE or a separate item could be included called Sharing Reduced Loss (SRL).

**KPI Approach**

The ALE method has the support of much of the existing literature, but a method that has been used in other non-revenue generating program evaluations like training, is the key performance indicator (KPI) approach. This method provides an analysis of ROI through statistically tracking performance metrics for investment initiatives over time to see whether investments have made a significant, positive impact on the organization. For example, because cybersecurity investment is supposed to improve security and efficiency, we can see whether the new identity and authentication management system (IAM) led to a decrease in metrics like, number of stolen accounts, data breaches, etc. In this case, implementation of an IAM system is our key independent variable, while stolen accounts, number of data breaches would be examples of possible dependent variables. Based on the statistical model chosen, other independent variables would be considered to take into account all possible changes on the chosen dependent variable. These other independent variables could include type of account (employee, contractor), experience of the employee, training of the employee, regional or geographic factors (rural, urban), etc.

Each organization that conducts a KPI based ROI analysis will have different key performance indicators depending on their business mission, industry, and general maturity level. For example a large manufacturing company with thousands of employees, an IT department, and a large budget for cybersecurity will have different indicators compared to a rural electric organization that has a small staff and must also consider sector specific regulation. Below I
have outlined some potential KPIs that may be part of many cybersecurity ROI analyses using this method, but each organization should consider their own specific situation.

To start, Initiatives that are part of a cybersecurity program should be reviewed and KPIs that could potentially demonstrate improvements will be determined.

Potential Initiatives:

- Improving the security of accounts (stronger passwords etc)
- Upgrading technology (firewalls, monitoring, etc)
- Providing additional cybersecurity training for employees
- Improving policies and procedures

KPIs:

An individual cybersecurity program will have to be researched and analyzed to ensure the selection of the best metrics and KPIs to represent their ROI. Below is an example process of how this would be done:

1. Understanding Programs – Research program functions and objectives while aligning the program objectives with cyber risk initiatives
2. Data Exploration – Investigate the data currently available from the organization and other sources and assess the likelihood of turning into a KPI metric. The data usability will be evaluated against following criteria:
   - Relevance to cybersecurity initiatives – KPIs must relate to cybersecurity initiatives and associated program goals. Returns based on such KPIs will be considered as return on security investment.
   - Monetization Potential – ROI calculations require KPIs that can be converted to a monetized value. KPIs that have monetization potential and utilize either organization benchmarks or industry and government-wide standards will receive priority.
   - Data Quality and Data Granularity – This metric will be assessed on its reporting frequency and timeframe, facility granularity level, consistency in reporting process, and severity of gaps.
3. Outreach will be conducted based on the criteria above to determine KPI alignment and availability.

4. Determine and verify the priority of the KPIs for analysis

Potential KPIs an organization could consider are:

- Number of data breaches
- Number of stolen accounts
- Compliance with relevant regulatory regimes or standards
- Bandwidth to survive DDoS attacks

Segmentation and Prioritization

Before the ROI can be determined from key performance indicators, information must be gathered and used to segment and prioritize programs and initiatives. Depending on the organization and the complexity of security in the organization, gathering data can be very challenging. To ensure good data is used in the analysis, the data should come from a number of sources within the company and external to the company. In addition to a variety of sources, the data should be collected at multiple times to try and ensure accuracy. After the data has been gathered on the programs and indicators that were selected, they can be segmented based on the data that was received.

One basic option for segmentation would be to create groups around initiatives where analysis is possible and a group where the data was not complete enough so analysis cannot be done. It is important to focus on initiatives where the data is complete so the ROI analysis can be based on evidence as much as possible versus incomplete pieces.

Analysis

After segmenting and prioritizing the initiatives and the KPIs, the organization can use a number of different ways to conduct analysis including a basic multivariate regression model. This regression analysis would show that for each additional specific investment in cybersecurity, the organization could expect an X percent reduction in successful attacks or Y percent reduction in stolen accounts. This model would include control variables to include general economic
conditions and changes in the security environment.

An additional potential way to look at the data is to use a Structural Equation Model (SEM) which is a statistical method of testing and estimating the causal relationship between variables. In an ROI analysis for cybersecurity, all of the factors and available measures of these factors would be laid out in a path diagram showing the potential cause and effect linkage among all variables. A new firewall was put in place during a time of higher attacks across the industry or economy as a whole which reduced the number of successful attacks. The SEM can be used to show potential paths and then continued testing can confirm or deny these paths.

After a relationship was shown between the particular investment in cybersecurity and specific KPIs the organization chose the challenge becomes to try and monetize the change in each KPI. This is a greater challenge in cybersecurity because of the lack of actuarial data and wide variety in estimates, but similar to the ALE model it can be done. For example, if a particular type of successful attack, DDoS, is a KPI the organization is interested in then the change in that number can be monetized based on historical costs of a successful DDOS attack.
Final Remarks

Trying to determine the ROI of cybersecurity investments is extremely challenging as there is very limited historical data and the results of an attack are rarely easy to see. But cybersecurity is becoming more important to many different types of organizations who are trying to benefit from the increased connectivity of many devices. To serve this need, technology has developed with clear security benefits, but what is the right amount of security and which technology will work with existing infrastructure? Because cybersecurity itself does not create new revenue, the basic ROI model of comparing the financial return to the financial cost of the investment does not apply. Academic research has changed the model to focus on the potential loss prevented which works well for how cybersecurity is viewed by most organizations. In addition to the ALE model, a proposal that comes from other ROI evaluations of non-revenue generating programs is the KPI model which uses indicators to represent changes in the organization caused by the investment. Ultimately each organization has a different level of security and will look for a different return on their investments. One organization may have very advanced security and looks to add a small piece that may not have a huge return but will eliminate an area of concern while a different organization may have very little in terms of cybersecurity and the first investment may have a very large return.

Differences in organizations and their risk management and security needs is another reason why creating a standard return on security investment model is challenging or impossible, but organizations should continue to try and define their return. This effort will allow an organization to understand their security and systems better in addition to thinking of cybersecurity in a business sense which is the goal of the NIST Cybersecurity Framework and other cybersecurity efforts. Another benefit of trying to define the returns is that models will improve as more actuarial data will become available so the monetization of cybersecurity returns should get more accurate. Overall with the increase in threats and attacks organizations will be looking for better cybersecurity and they will make investments to achieve this. Organizations that can make better investments to create better security and save money will end up being more successful while organizations who cannot determine their return are in danger of not surviving.