



Interested in learning
more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Quantifying Business Value of Information Security

been difficult to measure. For this reason some organizations forgo implementing security controls that could bring a positive return on investment to their organization. The goal of this paper is to familiarize the reader with risk management terminology, discuss how it can be applied to risk management and budgeting situations and present a quantitative risk management valuation process to show the benefit of a security control to the business. Using the methodology outlined in this paper the reader will be able t...

Copyright SANS Institute
Author Retains Full Rights

AD

Enhance security with
Entrust Unified Communication Certificates



Quantifying Business Value of Information Security Projects

GSEC Gold Certification

Author: Eric Poole, epoole@sonnenschein.com

Adviser: Jim Purcell

Accepted: July 20, 2009

Outline

- i) Abstract
- ii) Introduction
- iii) Overview of the quantitative risk management process
- iv) Determining Asset Value
- v) Types of loss
 - (a) Business loss due to reputation impact
 - (b) Productivity
 - (c) Rework
 - (d) Legal
- vi) Quantifying the value of a project
- vii) Conclusion
- viii) Risk Management Terminology
 - (1) Single Loss Expectancy
 - (2) Annual Loss Expectancy
 - (3) Annual Rate of Occurrence
 - (4) Modified Annual Loss Expectancy
 - (5) Return on Security Investment
- ix) Appendix I - Risk Management Terminology
- x) References

1. Abstract

The value that Information Security brings to an organization has traditionally been difficult to measure. For this reason some organizations forgo implementing security controls that could bring a positive return on investment to their organization. The goal of this paper is to familiarize the reader with risk management terminology, discuss how it can be applied to risk management and budgeting situations and present a quantitative risk management valuation process to show the benefit of a security control to the business. Using the methodology outlined in this paper the reader will be able to better describe to a business what the impact of security controls are on the bottom line of the organization.

2. Introduction

Does a company's investment in information security increase the value of a company? If so, how do you measure and articulate this value? Is a company better off investing in industry standard information security practices or striking out on its own and investing based on internally developed principles? How does this investment principle change if the company is unregulated or lightly regulated? To answer these questions this paper will discuss topics such as asset valuation, types of losses and risk management terminology. The reader will be presented with a quantitative project assessment model that applies the topics discussed in this paper to demonstrate how information security can be used to decrease the risk and cost of business operations. A Bruce Schneier quote that eloquently states several of the benefits of a quantitative, formalized project valuation process is as follows; "You can't completely remove emotion from risk management decisions, but the best way to keep risk management focused on the data is to formalize the methodology. That's what companies that manage risk for a living -- insurance companies, financial trading firms and arbitrageurs -- try to do. They try to replace intuition with models, and hunches with mathematics." (Schneier, 2009) The quantitative project assessment process presented in this paper is designed to do just that - formalize the methodology and focus on the data.

3. Overview of the quantitative risk management process

The purpose of a quantitative risk analysis is to show in a standardized, repeatable and comparable way how a security control adds value to a business. The process begins with the selection of a risk to be mitigated and a mitigating security control. The security control can be a process or a technology. The implementation and ongoing operating costs are listed. The types of losses that could occur as a result of the business operation are listed and the estimated loss to the business before and after a mitigating security control has been introduced are calculated. By determining the estimated risk of loss before and after the security control has been implemented, the value added to the business (minus implementation and ongoing costs) is revealed. Based on this information the Information Security department is better able to quantify the business value of the work they do, compare the value of prospective projects and determine what work should be focused on to deliver maximum value to the business.

4. Determining Asset Value

The value of many systems is not fully realized until a failure occurs. Take email for instance, most of us take for granted the ability to email colleagues when collaborating on projects, scheduling meetings, etc. Only when email is not available do we realize the impact it has on the way we work. This leads us to one method of determining the value of an asset - by taking it away and estimating the impact to the business if the asset were to disappear, go offline or stop functioning without notice. In some cases a less cost effective workaround could be used in place of the usual system. Other times, an additional business cost or loss occurs until the functionality of the failed system or asset is restored.

In this example we will estimate the hourly value to the business of an eCommerce system for an online sporting goods store. The eCommerce site for this business is the primary interface through which customers can order products from the company. There is an 800 number that customers can call to place orders, request assistance with the site, etc but the eCommerce site is the only way they can view products (there is no catalog). Ninety-nine percent of the company's sales are done through the site. In the grid below are the company's revenue statistics for the previous year, along with the percentage of sales that were done through their eCommerce site.

eCommerce System	
Annual Sales Revenue	\$6,000,000.00
Percentage of sales through eCommerce	99%
Revenue generated through eCommerce site	\$5,940,000.00
Hourly Revenue (Annual Revenue from site/8760 hours in a year)	\$678.08

Some simple calculations based on the Annual Revenue and Percentage of sales through eCommerce tells us that the hourly value of the eCommerce site to the

business is \$678.08. This was found by multiplying the percentage of sales through eCommerce by the annual revenue ($.99 * \$6,000,000.00$), which results in the 'Revenue generated through eCommerce site' figure of \$5,940,000.00. The revenue generated through eCommerce is then divided by the number of hours in a year (8760) to arrive at the hourly revenue of the site. The resulting number (hourly revenue - \$678.08) can be used as a SLE for an hour of system downtime.

With the SLE determined in this exercise, the value of a high availability solution for the eCommerce system becomes clearer. Based on this information (along with ARO) a business is able to determine which security control is right for their needs.

5. Types of loss.

There are several types of loss that companies can experience as a result of a security incident. Four of these loss types will be defined below and applied later in this paper when the template for quantifying business value of a project is discussed.

- Productivity - productivity lost due to a security incident can be seen in several ways; downtime for an end user while the application they need to work in is down or time spent by an employee surfing the internet instead of working. This type of loss is easy to quantify. Productivity lost due to an hour of system downtime can be calculated by taking the average salary of a user of that application and multiplying it by the number of hours the system was down multiplied by the number of users affected. Annual Rate of Occurrence (ARO) for this type of event could be calculated by reviewing past help desk tickets.
- Rework - security events can cause data corruption or data loss. For instance, in the event of a virus infecting a file server housing important company information. Investing in a high availability or backup solution for the data stored on these servers could mitigate the rework costs of recovering from a virus. This loss would require work to quantify but would not be difficult. While the rework costs to produce specific data should be easily quantified, the amount of data that could be damaged by malicious code could range from one file to several servers.
- Legal - Legal fees and potential additional liability costs from lawsuits.

An example of this type of loss can be seen in the recent data breach at TJ Maxx. In this case the company is facing a lawsuit from several banking groups; “In a lawsuit pending in US District Court in Boston, the Massachusetts Bankers Association and trade groups from other states seek unspecified recovery for damages they describe as being “in the tens of millions” of dollars for the costs related to replacing compromised cards.” (Kerber, 2007) Even if TJ Maxx wins the court case, they will have had to invest significant funds in their legal defense team as well as suffering additional reputational impact from the data breach story having spent additional time in the newspaper headlines. This type of loss is difficult to quantify. The number of lawsuits, hours invested in each and potential judgments against the business are all highly variable depending on the specifics of the event. Even sources such as the Data Theft Loss calculator (Darwin Professional Underwriters, 2007) decline to estimate the cost of civil damages resulting from a data breach, due to limited data. Clearly legal costs of a data breach are difficult to predict and are subject to high variability.

- Business loss due to reputational impact -An example of this type of loss would be a customer who no longer shops at TJ Maxx due to their highly publicized data breach. This loss is difficult to quantify. Business impact of customers reacting to a security event (data breach in this case) is difficult to predict. Several factors such as publicity, severity of the event and resulting detrimental impact to customers are all highly variable and difficult to predict. Due to the lack of information and variability of impact this type of loss could be considered more qualitative than

quantitative.

6. Quantifying the value of a project

In this section a spreadsheet applying the risk management formulas discussed throughout this paper will be presented to help quantify the value of a security control. By using a standardized, repeatable process to judge project proposals based on the same criteria, it is possible to eliminate emotion and misconceptions from the project valuation and selection phase. It is important to keep in mind throughout this process that "the point is to provide a set of guiding principles from which (the business) can make good decisions about what's acceptable. In other words, the CEO doesn't (or shouldn't) care if a return is precisely \$3.13 for every \$1 spent or \$2.97. He cares that it's accurate to suggest about a 3-to-1 return, and not a 1-to-1 return or, worse, a 1-to-3 return." (Berinato, 2002) SLE and ARO estimates are often times overanalyzed when there is no perfect answer. The goal here is to make a reasonable estimate based on the data available. Even if the estimates of SLE or ARO are imperfect, all proposed projects are still judged by the same standard which should produce an accurate comparison of relative value between the projects.

This project valuation spreadsheet will use the example of an anti-virus project for workstations and servers in an enterprise. The cost and benefit sections of the spreadsheet are shown at the end of this section, along with a brief discussion of how the risk assessment formulas discussed in this paper are applied.

The cost section of a project valuation spreadsheet lists implementation and ongoing costs of the project including:

- Server hardware and software costs - these specifications can

usually be obtained from vendor documentation.

- Implementation labor - the hours of employee labor needed to complete a company-wide implementation of the anti-virus solution. Consulting hours if needed can be included in this section as well. The hours of labor needed is then multiplied by the average hourly rate of employees on the project to determine the labor cost of implementation. In this example \$50 per hour has been used as the hourly rate for employee labor.
- Ongoing labor - the hours of labor of employees needed to maintain the functionality of the anti-virus solution on an annual basis. The hours of labor needed is then multiplied by the average hourly rate of a systems administrator that would be maintaining the system.

The benefit section of the spreadsheet calculates the cost savings from the decrease in various business losses as a result of the project. For example, the Decreased Employee Productivity Loss section shows calculations that demonstrate how the ARO of anti-virus incidents decreases as a result of the anti-virus system, resulting in a productivity increase for the business. The acronyms used in this section are defined in Appendix I.

- ARO - the number of virus infections resulting in user downtime each year. This number could be estimated based on historical data found in help desk tickets from previous years.
- SLE - the SLE is the estimated cost to the company for each instance of this incident. Here we are estimating that the end user will

experience 30 minutes of downtime on average and that the help desk will also spend 30 minutes between troubleshooting or reimaging the workstation.

- ALE - the ALE is calculated by multiplying ARO and SLE. This determines the annual loss due to this type of event.
- mARO - this is an estimation of ARO once the security control has been implemented.
- mALE - this is an estimation of ALE after the security control has been implemented.
- Productivity cost savings per year - mALE minus the ALE. This is the value of the security control in decreasing productivity loss.

The cost savings calculation is repeated for each type of business loss the project is expected to address. The mALE estimates are then added together to determine the total cost savings as a result of the security control, this result is shown in the 'Total Cost Savings' field of the spreadsheet.

Once the costs and benefits of the project have been calculated, RoSI can be determined by subtracting the costs of the project (\$22,500 for the first year, including implementation costs) from the mALE (Total Cost Savings of \$410,000) which results in \$387,500.00. It is much easier to present a project proposal to the business when you can show that the project has significant RoSI for the business. Additionally, presenting this in spreadsheet form allows changes to be made on the fly and the impact of these changes to be seen quickly. For instance there may be other projects or outside factors brought up by management that would impact the ARO or SLE of the risk addressed by the project. Changes made to these

estimates can be made easily and their effect on the value of the project is immediately seen.

Benefits			
Decreased Employee Productivity Loss			Decreased time lost by end users
Annual virus infections resulting in user downtime (ARO)		3750	
SLE (estimated cost of 30 minutes of end user downtime plus		\$50.00	
ALE		\$187,500.00	
mARO		750	
mALE		\$37,500.00	
Productivity Cost Savings per year		\$150,000.00	
Decreased Rework			Decreased reimages of PCs, recreation of corrupted files
Hours of work list per year (ARO)		2250	
Average Hourly Rate (SLE)		\$50.00	
ALE		\$112,500.00	
mARO		\$750.00	
mALE		\$37,500.00	
Decreased Rework Cost		\$75,000.00	
Decreased Legal Fees			Decreased Legal fees due to data breach
ARO		0.05	
SLE		\$6,600,000.00	
ALE		\$330,000.00	
Modified ARO		0.025	
Modified ALE (mALE)		\$165,000.00	
Decreased Legal Fees		\$165,000.00	
Decreased loss of business from security incidents			
ARO		0.02	
SLE		\$2,000,000.00	
ALE		\$40,000.00	
mARO		0.01	
mALE		\$20,000.00	
Decrease in lost business		\$20,000.00	
Total Cost Savings		\$410,000.00	
Costs			
2 Servers	\$4,000		
2 Windows Server Standard Edition Licenses	\$400		
Implementation Labor (in hours)	262		
Hourly Rate	\$50		
Implementation Labor Cost	\$13,100		
Total Implementation Cost	\$17,500		
Yearly Labor to Maintain (in hours)	\$100		
Hourly Rate	\$50		
Yearly Cost	\$5,000		

7. Conclusion

Demonstrating the value that Information Security brings to a business is not always a simple task. In this paper several risk management formulas have been discussed that can be helpful in estimating the risk exposure of business operations and the mitigating value of security controls. A process was discussed for presenting risk management estimates in the form of a spreadsheet which helps present the information in a clear, uniform format and allows for changes to be made on the fly to ARO, SLE or other variables with the impact of these changes on risk exposure to be seen immediately.

It is often useful to go through the exercise of determining the business value of information security not only when proposing a new project to the business but also as a review of what value existing Information Security tasks, systems, services, and other deliverables provide to the business. By matching up information security work that produces the highest positive RoSI and helping the business understand the real value of security controls you will be improving the chances for long term success of your business.

8. Appendix 1 - Risk Management Terminology

Certain terms used when discussing risk management and the value of information security are fundamental to the topic. Several of these terms are defined in the following section.

SLE (Single Loss Expectancy): SLE is the expected loss from a single instance of an event. This can be based on historical data of previous incidents or if the event has never before occurred, it can be estimated. An example of SLE would be the cost to a business from a virus infecting an end users laptop and the resulting productivity loss to the user, time investment from the IT department to either clean the machine or reimage it, as well as time invested by IT to ensure the virus has not spread to any other systems in the enterprise (IDS event analysis, event log analysis, anti-virus report analysis).

ARO Annual Rate of Occurrence): ARO is the estimated annual frequency of an incident. This can be any positive number, including numbers less than 1. For instance, if a particular event was estimated to occur once every 10 years, the ARO would be 0.1. An example of this would be number of times an end user PCs becomes infected with a virus every year. This figure could be found by looking at help desk tickets from previous years.

ALE (Annual Loss Expectancy): ALE is the result of $SLE * ARO$. By multiplying the expected loss from a single event by the number of times it is expected to occur in a year, the expected annual loss from this type of event can be calculated.

mALE (Modified ALE): mALE is the ALE after mitigating actions have been

taken to reduce the risk of an event. The value a business receives by taking countermeasures to reduce risk can be demonstrated by subtracting mALE from ALE. (Berinato, 2002)

RoSI (Return on Security Investment): RoSI can be figured by subtracting the mALE (savings to the business from mitigating actions taken to reduce risk) from the costs of the security control, both implementation and ongoing annual costs to maintain the control. This results in the amount the business saves (or loses if the RoSI comes out as a negative number) as a result of implementing the security control. (Berinato, 2002)

9. References

1. Schneier, Bruce. "Does Risk Management Make Sense?" Retrieved April 24, 2009, from Does Risk Management Make Sense?;
<http://www.schneier.com/essay-240.html>.
2. Schneier, Bruce. "Security ROI Fact or Fiction" Retrieved April 24, 2009, from Security ROI Fact or Fiction;
<http://www.schneier.com/essay-237.html>.
3. Berinato, Scott. "Calculated Risk: Return on Security Investment " Retrieved April 24, 2009, from Calculated Risk: Return on Security Investment;
http://www.csoonline.com/article/217727/Calculated_Risk_Return_on_Security_Investment
4. Kerber, Ross. "Cost of data breach at TJX soars to \$256m" Retrieved April 25, 2009, From Cost of data breach at TJX soars to

\$256m;

http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/.

5. Darwin Professional Underwriters (2007). “Tech//404 Data Loss Calculator” Retrieved May 9, 2009, From Tech//404 Data Loss Calculator; <http://www.tech-404.com/calculator.html>.



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced