

A NetClarity, Inc. White Paper



NetClarity, Inc.
54 Middlesex Turnpike, Building C
Bedford, Massachusetts, USA 01730
Tel: 781-276-4555
Fax: 781-276-1569
<http://www.netclarity.net>

Is There an ROI to Network Security?

*By Gary S. Miliefsky, CISSP®
Founder & CTO*

2007 Edition

Contents

Introduction	3
The ROI Formula	3
The Risk Formula	4
Real-World Scenario	4
Credits	5
About the Author	6
Copyright Notice	6
Contact Information	6

Introduction

Can we find an ROI in Network Security?

The ROI Formula

Know this formula and you're on the right track.

The Risk Formula

Incorporating risk into the equation will help you create a Network Security ROI formula.

Real-World Scenario

Let's see these formulas in action and prove there is an ROI to Network Security.

INTRODUCTION

There's a very strong argument that Network Security costs boat loads of money and provides no return on investment. Your CFO might be convinced that the IT equipment purchases as well as IT staff time spent configuring and managing your entire network is just another hefty cost of doing business. When it comes to network security in particular, the CFO is probably even more certain that it's a big expense with no return. It's probably looked at as some kind of costly insurance policy to help show that you both are taking necessary measures to protect your business.

The argument might be "when did an alarm system or the lock on the front door return money back to us?" These are physical security measures that everyone has to take in due care to keep intruders out or help keep honest people honest. Ok, so you could claim it returned a little bit back to you, because you received a discount on your insurance policy for proactively taking these simple precautions to keep out the intruders. But is there an ROI to spending thousands on insurance and saving only a few hundred bucks for having bolted your doors and alarmed your windows?

Knowing that organizations spent over \$10B USD worldwide on

Network Security equipment over the last few years, this argument that there is no ROI - it's just a cost of doing business starts to sound like it has merit. In fact, even after spending all this money, so many organizations experienced expensive downtime - due to hackers, viruses, worms, spyware, spam and malicious insiders. So, where's the ROI in Network Security?

THE ROI FORMULA

In mathematical terms, the arithmetic return of ROI is defined as the following:

$$ROI_{Arith} = \frac{V_f - V_i}{V_i} = \frac{V_f}{V_i} - 1$$

This return has the following characteristics:

$ROI_{Arith} = +100\%$ when the final value is twice the initial value

$ROI_{Arith} > 0$ when the investment is profitable

$ROI_{Arith} < 0$ when the investment is at a loss

$ROI_{Arith} = -100\%$ when investment can no longer be recovered

Interestingly, to compensate for a negative ROI, one needs a positive ROI that is higher in magnitude. For example, to recoup a 50% loss one needs to realize a 100% gain (source: Wikipedia.org).

A simpler formula for ROI that takes into account annual returns is as follows (source: NucleusResearch.com):

ROI = ((net year 1 + net year 2 + net year 3) / 3 / initial cost) X 100%

So, typically, ROI is looked at by the monies generated as net income. If you spend money on equipment, usually there's a total cost of ownership (TCO) attributed but not an ROI, or better yet, the ROI is below 100%, so it's a loss not a profit. As a result, this kind of equipment can get written off over time as a capital expenditure - in other words a 'cost center.'

Here's an example using the simple formula around hiring a sales person who goes out in the field and generates a net income for his company. Let's say the TCO for this employee is \$100k per year (salary, bonus, overhead), he brings in a net of \$100k, \$150k and \$200k in revenues over a 3 year period):

ROI = ((\$100k + \$150k + \$200k)/3/\$100k) x100% so...

ROI = ((\$450k)/3/\$100k) x100%, which equals 150% - that makes sense, you spent 300k but it returned you 450k so the ROI is 150% which is good. If the ROI is below 100% then you are losing money. Makes sense, right?

Now that we've completed the ROI crash course, I'm going to turn the tables and show you that there is indeed a POSITIVE ROI

to Network Security. Before you can measure it to prove it to your CEO, CFO or the Board, first you need to have my crash course on risk assessment and then we'll tie it all together.

THE RISK FORMULA

My crash course on risk assessment is easy:

$$R = T \times V \times A$$

That is, (R)isk is equal to the number of (T)hreats against your organization, multiplied by the number of (V)ulnerabilities you have and then by the number of assets.

Threats, Vulnerabilities and Assets are all weighted by how serious the threat, vulnerability and how valuable the asset.

REAL-WORLD SCENARIO

Here is a for instance: What is the risk that your salesperson will not meet his quota of \$100k in year one, \$150k in year two and \$200k in year three from the example above if at the end of every quarter, the mail server goes offline, the network fax server won't send out quotes and invoices or accept inbound purchase orders because these servers were operating in a Risky environment that was constantly hammered by hackers, viruses and worms (Threats) which were easily exploiting the weaknesses in your network (Vulnerabilities) and taking these servers offline (Assets). At that moment

in time, productivity dropped, revenues couldn't be booked and the ROI for sales fell below 100%.

So what do you do to get this sales person's ROI over the 100% mark, you implement strong Network Security by creating policies about who can come and go in your network and what kind of traffic can flow to and from these critical assets. In addition, you deployed apparently costly network security equipment like firewalls, vpns, ids systems, anti-virus, anti-spam and anti-spyware. You began to more frequently self-audit your own Risk profile until you reduced your level of Risk to an acceptable level - no more mail and fax server downtime.

Now, let's say you had 100 sales people bringing in 150% and the TCO of Network Security is now factored into this equation:

ROI = ((net year 1 + net year 2 + net year 3) / 3 / initial cost) X 100%

ROI = ((\$10M + \$15M + \$20M)/3/[\$10M TCO Sales team + \$2M TCO CIO's Team and all Network Security expenditures]) x100% so...

ROI = you spent 12M but it returned you 15M so the ROI is 150% which is good.

Let's take away Network Security and now factor in downtime, lost productivity, unhappy customers and lost revenues:

ROI = ((\$10M + \$9M + \$8M)/3/\$10M TCO Sales team only) x100% so...in this case your ROI is 90%. You spent only \$10M, shaving \$2M by not having the CIO, IT Staff and Network Security expenses, but your risk was high and the experience of downtime cost you important revenues. As a result you earned \$9M and spent \$10M on average. What does that do to your business? It puts you out of business.

There is absolutely an ROI for good Network Security.

What is the end result of your actions?

Ultimately, by investing up front in best practices and the necessary tools for good Network Security, you were able to ensure higher revenues and profitability. Doing it right means more uptime, more productivity and smoother sailing through each quarter.

CREDITS:

Thanks to numerous NetClarity, Inc. customers for their time and suggestions for this document. Thanks also to <http://www.SearchCIO.com> for providing information on their web sites and for publishing my short article on this topic.

About the Author:



Gary S. Miliefsky, CISSP®

Founder & CTO
NetClarity, Inc.

Gary Miliefsky has 20+ years experience as an entrepreneur, computer scientist and trained security professional. He has been CEO and/or CTO of 3 start-up ventures.

Mr. Miliefsky is a founding member of the Department of Homeland Security, <http://www.usdhs.gov/>. He currently serves as an advisor to MITRE Corporation at <http://oval.mitre.org/> and is a member of the New England Information Security Group's Board of Directors, found at <http://www.neisg.org/>. He received his undergraduate degree from UMASS Lowell in Computer Science and subsequently earned certification as a CISSP®.

Mr. Miliefsky holds six e-commerce patents and has seven network security patents pending, including one about Proactive Network Security Using RSS. He maintains a Blog about IT Security Tips, Trends and News at <http://netclarity.blogspot.com>.

COPYRIGHT NOTICE:

All rights reserved. Printed in the United States of America. No part of this Whitepaper may be reproduced in any form and by any means without prior written permission of NetClarity, Inc. Making copies for any other use than backup purposes is a violation of US and International copyright laws. Copyright © 2006, NetClarity, Inc.

CONTACT INFORMATION:

Feel free to visit Gary online at <http://www.netclarity.net>. If you have any questions about this paper, please send an email to support@netclarity.net.

NetClarity, Inc.
54 Middlesex Turnpike, Building C
Bedford, Massachusetts, USA 01730

Tel: 781-276-4555
Fax: 781-276-1569
SKYPE: netclarity

Web: <http://www.netclarity.net/>