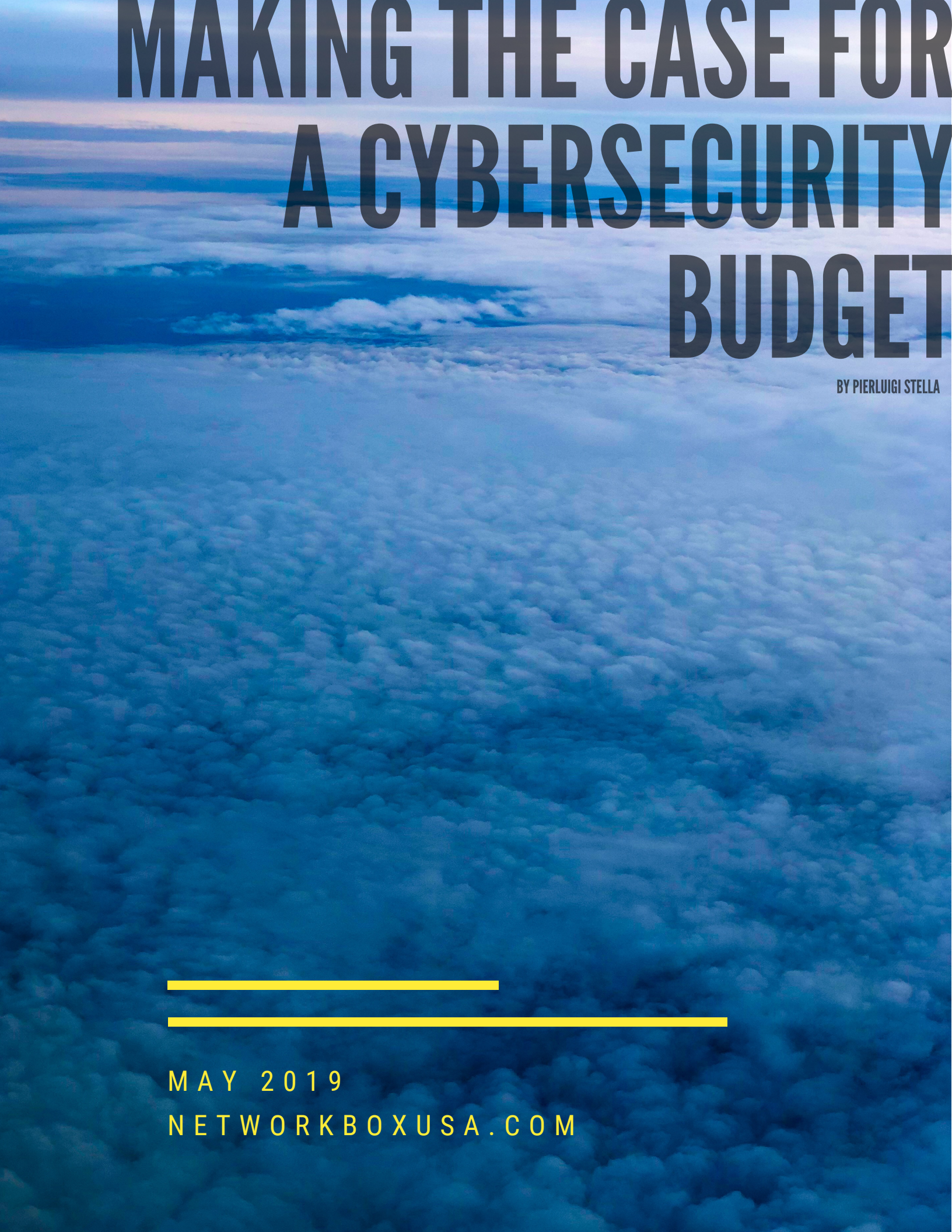

MAKING THE CASE FOR A CYBERSECURITY BUDGET

BY PIERLUIGI STELLA

MAY 2019

NETWORKBOXUSA.COM

How do you start to calculate the cost of poor security?

why do you even need money if nothing has actually happened?

"I don't understand what you're saying, security doesn't affect profits"

IS SECURITY AN EXPENSE?

While 15 years ago security was being seen as a nuisance, or maybe a necessary evil, this view has evolved over the years and today security has become a very important business unit. One that's on a par with marketing and sales, because without security, companies cannot even begin to exist.

The most common objection we receive when discussing budgets with C-suites is "*Why do you need more money if nothing has happened?*", or worse, "*Why do you even need any money if nothing has happened?*".

We need to start by changing our own mindset. We need to stop viewing security as an expense. We aren't a cost center. And yes, in a way, we're a form of insurance, but you can't approach the conversation in that manner because insurance is **still** a cost and doesn't produce revenue.

OR IS SECURITY A FORM OF INSURANCE?

Showing the Total Cost of Ownership (TCO) is also not a good approach. We're still talking about cost, and we've said that's not a good approach. Furthermore, in order for the actual TCO of a security solution to be properly evaluated, it must also include "*your*" time. If you don't factor that in, your CEO certainly will, at which point, you would've yourself become a cost. And costs **always** need to be reduced.

The language CEOs know all too well is one of ROI and profitability. That's where the conversation needs to go.

From its definition (**ROI = Net Profit over Total Investment times 100 or NP/TI * 100**), ROI must be greater than 100 or we've lost money.

Our job is to demonstrate that the ROI of cybersecurity investments is greater than 100. That there is **indeed** a Net Profit to this equation.

SECURITY IS NO LONGER TCO BUT ROI

We know that gross profit margin is defined as:

((**Revenue – Cost of goods sold) / Revenue)** X 100

A positive ROI contributes to the gross profit margin by either increasing the revenue or decreasing the cost it took to produce that revenue. Cost reduction is achieved as cost avoidance – if you don't get attacked, you don't incur recovery costs, which can very quickly escalate.

To cite a well-known attack that was in the news for a period of time (*towards the end of 2013*), Target lost $202M. Between loss of records, notifications to clients, forensics, image, loss of revenue, loss of stock value (*and more*), the retail giant lost 46% of revenue for the season.

Could **your** company survive such a hit?

RETURN ON SECURITY INVESTMENT

So now the burden is on us to determine how much a security incident could cost the company. For starters, 60 percent of small organizations that suffer a cyber-attack end up going out of business within 6 months. Now, **THAT's** a cost!

There's actually a formula to calculate the return on security investments, as proposed by the SANS institute:

ROSI = (**ALE x Mitigation Ratio – Cost of solution**)/ Cost of solution

ROSI means Return on Security Investment.

ALE means Annualized Loss Expectancy and represents the estimated amount of money that could be lost in a single security incident, multiplied by the estimated frequency that a threat will strike within the same year.

HOW MUCH WILL A BREACH COST YOU?

Mitigation Ratio is an approximate number, and it's based on mitigation factors that depend on actions the company is taking to reduce a risk *(i.e. having real time backups vs daily backups*).

Cost of the solution is clearly what you'll spend to avoid the risk altogether.

High costs can ultimately negate the value of the solution, if the ROSI ends up being lower than one.

What do you evaluate as part of cost avoidance?

What is the cost of poor security?

That answer relies heavily on your company, and also on the type of industry you operate within.

WHAT IS THE POTENTIAL LOSS OF NOT HAVING SECURITY?

In general, you'll need to consider the time spent diagnosing and fixing the issues; the time your employees will spend idling because they don't have a computer to work; loss of productivity; cost of IT personnel to fix issues and improve overall security so the incident doesn't reoccur; cost of new security solutions; cost of forensics analysis, especially when it's legally mandatory; and let's not forget also the cost of loss of image, which can be incalculable sometimes.

If you're providing something that's like a commodity, loss of image triggered by a security incident can compel your clients/customers to approach a competitor, and they may never ever return to you.

Even for small companies, where potential loss is usually <$50,000 per incident, the frequency at which an incident can reoccur irrefutably justifies large ROSIs.

OR WHAT IS THE POTENTIAL GAIN OF HAVING SECURITY?

Cybersecurity may seem like a cost; but an attack is undeniably a cost, and it can be a large one. Large enough to send you out of business (*since the larger you are, the larger your corresponding expense and cost*). How many small and medium companies (*and frankly even large companies*) have the cash reserves to continue operating in the face of a 46 percent revenue loss for several consecutive months?

It should be clear from all this that proper cybersecurity delivers ROI in the form of cost avoidance. And that the avoided cost, albeit an estimation, can truly be very high.

Another way of showing that security contributes to the profitability of a company (*that it delivers positive ROI and contributes to the revenue, thereby increasing the profitability of a company*), is by understanding that in 2019, it has become virtually impossible to do business without proper security.

SECURITY IS NOT A NECESSARY EVIL

Being able to demonstrate to business partners and clients alike that you take cybersecurity seriously is a clear business advantage. In this day and age, it's inconceivable to do business if you can't show proper cybersecurity. Fact of the matter is, companies have learned to do due diligence on their vendors and partners. What this means is that aside from checking financial reports and other aspects of the business itself, they're also reviewing the security posture of their business partners.

In a nutshell, without adequate cybersecurity in 2019, you cannot hope to conduct business and be successful.

Security is no longer something you undertake grudgingly. Security is an important, integral part of every sound company intending to be in business for the long haul.

SECURITY IS A BUSINESS ADVANTAGE

Security delivers a **POSITIVE ROI** based on the simple fact that without security, there simply is no company. Without security, there's no revenue. In truth, across many instances, there's no business without security.

Why?

Because in a time when far too many companies are still not taking the matter seriously, proper cybersecurity provides a real business advantage, and a truly unique differentiating factor.

In conclusion, it's high time we all stopped viewing ourselves as a cost center. As some kind of necessary evil.

Instead, let's consider that cybersecurity is now indeed a profit center, a business unit without which a company might not even exist.

MAKING YOUR CASE FOR HAVING A CYBERSECURITY BUDGET

When asking for a budget for your department, don’t be shy. Don’t think of it as an expense the company may not be able to afford, but instead as a vital investment the company simply cannot afford to do without.

Demand the best, and expect to be heard because without you, without cybersecurity, your company would quickly cease to exist.

You’re most definitely not a nuisance.

You’re a fundamental part of the business.

If you'd like more information on how to redefine your IT approach and build a cybersecurity budget that's realistic, balanced, and effective, please contact us. We'd be most happy to share our insights and knowledge with you.