NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

In the Boxing Ring NOV 2022

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the November 2022 edition of In the **Boxing Ring**

This month, Network Box USA's Chief Technology Officer, **Pierluigi Stella**, is talking about how to ask management for a cybersecurity budget and make your business case. Today, cybersecurity has become a critical business necessity. Without this, companies cannot function, let alone thrive. On pages 2 to 3, he provides the reader with ammunition to speak the language of and resonate with C-suite-level executives to ask for a cybersecurity budget.

In other news, Network Box won two BizIT Excellence Awards for outstanding performance in the **Unified Threat Management** and **Managed Security Services** categories. Furthermore, Network Box Germany was at the **ServerEye Partner Day 2022**. And in this month's global security headlines, security issues were found with **Fortinet**, **VMware**, and **Cisco** products.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
November 2022

Stay Connected

You can contact us here at Network Box HQ by email:
nbhq@network-box.com,
or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox

In this month's issue:

Page 2 to 3

Cybersecurity Budget: making your business case to management

In our featured article, Network Box USA's Chief Technology Officer, Pierluigi Stella, talks about how to ask management for a cybersecurity budget. When asking for a budget, do not consider it a cost; cybersecurity is a fundamental part of the business - without it, your company may quickly cease to exist.

Page 4

Network Box Highlights:

- **BizIT Excellence Awards**
  - Unified Threat Management
  - Managed Security Services
- **Network Box Germany**
  - ServerEye Partner Day 2022
- **Global Security Headlines:**
  - Sophos
  - VMware
  - Cisco

CYBERSECURITY BUDGET

Making your business case to management

by Pierluigi Stella
Chief Technology Officer
Network Box USA

In the past, cybersecurity has often been perceived as a nuisance, a necessary evil even, but this view has evolved over the years. Today, cybersecurity has become a critical business necessity, right up there alongside marketing and sales, requiring a budget of its own. Why? The reason is clear. Without cybersecurity, companies cannot function, let alone thrive. It is of immense importance, particularly when making the case to get the budget you need to achieve a robust security posture for the company's network. This article aims to provide the reader with ammunition to speak the language of and resonate with C-suite-level executives.

Let us begin by acknowledging that it is high time for a mindset change

By that, I mean that security people need to start changing how they think of themselves and their roles in the company.

The most common objection we hear when discussing the budget with management is, *"Why do you need more money if nothing has happened?"* or worse yet, *"Why do you even need any money if nothing has happened?"*.

We must start by changing our mindset and realizing that security is not an expense. We are not a cost center. We are, in a way, a form of insurance, but we do not approach the conversation from that angle since insurance is a cost, and it does not produce revenue.

Showing the Total Cost of Ownership (TCO) is also not a good approach because we are still talking about cost (we've already discerned how that's not a good approach) but also, the actual TCO of a security solution, to be correctly evaluated, needs to include *"your"* time. If you do not factor that in, your CEO will. When he does, you have just become a cost – and costs always need to be reduced, so there is that.

The language CEOs understand is one of ROI and profitability

That's how conversation needs to go down. From its definition: ROI = Net Profit over Total Investment times 100 **(NP ÷ TI x 100)**

ROI must be greater than 100, or we have lost money. Our job is to show that the ROI of cybersecurity investments is greater than 100. That there is indeed a Net Profit to this equation.

We know that gross profit margin is defined as:
([Revenue - Cost of goods sold] ÷ Revenued) 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 do not get attacked, you do not incur the recovery costs, which can be very high.

To cite a well-known attack that was in the news for some time, **Target** lost US$202 million at the end of 2013. Between the loss of records, notifications to clients, forensics, company image, revenue loss, and loss of stock value, the retail giant lost 46% of revenue for the season.

Could your company survive such a hit?

If you do not get attacked, you do not incur the costs of an attack. So now the burden is on us, the security guys, to determine how much a security incident could cost our company. For starters, 60% of small businesses that suffer a cyber-attack end up going out of business within six months. Now, **THAT'S** a cost.

There is 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: Return on Security Investment

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

Mitigation Ratio: an approximate number based on mitigation factors that depend on the company's actions to reduce the risk (i.e., having real-time backups vs. daily backups).

Cost of the solution: this is what you will spend to avoid the risk altogether. High costs can ultimately negate the solution's value 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 depends a lot on your company and your industry. In general, you will need to consider the following:

- Time spent diagnosing the issues.
- Time employees spend idling because they do not have a computer to use.
- Loss of productivity.
- Cost of IT personnel to fix the issues and to improve security, so the incident does not recur.
- Cost of the new security solutions.
- Cost of forensics analyses, especially when laws and regulations require this.
- Loss of company image, which could be quite incalculable at times. If you are providing something that's perceived as a commodity, the impact caused by a security incident on your credibility factor may very well propel your clients/customers towards your competitor and never return.

Even for small companies, where the potential loss is usually under US$50,000 per incident, the frequency at which an incident can happen again does justify large ROSIs. Cybersecurity may seem somewhat like a cost, but an attack is clearly and irrefutably one, and it can be a large one. Substantially large enough to send you out of business. How many small and medium companies (and frankly even large ones) have sufficient cash reserves to continue conducting business even in the face of a 46% revenue loss for several months in a row?

Proper cybersecurity delivers ROI in the form of cost avoidance, and the avoided cost (albeit just estimated) can be very high across ***the entire company.***

Another way of showing how security contributes to a company's profitability is that it delivers positive ROI (it actually contributes to revenue, therefore increasing profitability). It has become virtually impossible to do business without proper security. Being able to show your business partners and clients that you take cybersecurity seriously has become a keen business advantage.

Nowadays, it is nearly impossible even to do business if you can't demonstrate proper cybersecurity measures. Companies have learned to conduct due diligence on their vendors and partners, and part of this encapsulates a review of financial reports and other aspects of the business itself and the security posture of prospective business partners.

Security has become non-negotiable

Security is no longer something undertaken grudgingly. It is an important, integral part of every sound company intending to stay in business for the long haul. Security delivers a positive ROI based on the simple fact that without security, there is no company. Security directly contributes to a company's revenue because, without it, there will likely be no revenue at all. This means that without proper security today, you will find it impossible to conduct business let alone achieve any measure of sustainable success.

Furthermore, proper cybersecurity provides a real business advantage and a true differentiating factor at a time when still far too many companies are not taking this issue seriously enough.

> **To conclude, let's all stop thinking of ourselves as a cost center and some kind of necessary evil. Let's consider that cybersecurity is now a profit center, a business necessity without which a company might not even exist. When asking for a budget for your department, do not be shy and do not think of it as a cost the company may not be able to afford. Demand the best, and expect to be heard because without you, without cybersecurity, your company would quickly cease to exist.**
>
> **You are not a nuisance. Cybersecurity is a fundamental part of the business.**

Network Box HIGHLIGHTS

BizIT Excellence Awards 2022

Unified Threat Management Managed Security Services

Network Box is very pleased to announce that the company won two BizIT Excellence Awards for outstanding performance in the **Unified Threat Management** and **Managed Security Services** categories.

The BizIT Excellence Awards recognizes innovative applications and solutions for businesses and enterprises. After a thorough review process, a select panel of industry experts determined the winners of this year's awards.

Network Box Germany

ServerEye Partner Day 2022

Network Box Germany was at the ServerEye Partner Day 2022, which took place at **Big Eppel**, Eppelborn, in the German state of Saarland.

During the event, Network Box Germany's Managing Director, Dariush Ansari, talked about cybersecurity awareness in the IT industry. As more companies conduct business online, it is essential to educate staff about security to be better prepared for cyberattacks.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Global Security Headlines

Cybernews

Fortinet's critical bug already exploited in the wild
LINK: https://bit.ly/3zxQ20j

The Hacker News

Multiple Campaigns Exploit VMware Vulnerability to Deploy Crypto Miners and Ransomware
LINK: https://bit.ly/3SPhT2V

The Register

Cisco AnyConnect Windows client under active attack
LINK: https://bit.ly/3zwULPY