How to Optimize Returns on Cybersecurity Investments?

www.marlabs.com
TABLE OF CONTENTS

1. Introduction ........................................................................................................................................................................ 1
2. Why Enterprises Struggle to Realize Return on Cybersecurity Investments .................................................................................. 2
3. Your Cybersecurity Booster Shot: Continuous Controls Monitoring .................................................................................. 3
4. How Continuous Controls Monitoring Can Transform Your Enterprise ............................................................................... 4
5. Cyber Observer+ Marlabs to Optimize Your Cybersecurity ROI .............................................................................................. 4
Introduction

This year, a group of hackers launched a ransomware attack on Colonial Pipeline, an American oil pipeline company. As a result, the company shut down over 5,000 miles of pipeline, disrupting fuel supply and airline operations on the East Coast. The company paid $5M in ransom to restart operations.

This isn’t a rarity. There have been 175 publicized ransomware attacks in 2021 alone. Studies estimate cybersecurity costs to reach $6 trillion this year, with data breaches costing enterprises $8.64 million, on average. There are newer and more complex cybersecurity threats arising each day.

- 90% of healthcare organizations report at least one breach in the last three years.
- US citizens reported over 1.4 million identity thefts in 2020, almost double the previous year — this goes to show that rapid digitization is also accelerating security threats.
- 95% of attacks on enterprise networks happen through spear phishing.
- Despite the seriousness of risks, the likelihood of catching and prosecuting a cybercriminal is at a grand 0.05%.

Cybersecurity threats are omnipresent, unpredictable, and expensive.

Therefore, it’s no wonder that cybersecurity is growing to be a massive concern among leaders — US President Joe Biden is investing in strengthening its cybersecurity posture. Business leaders are doing so too. Nearly every business leader surveyed increased their cybersecurity investments in 2020.

Yet, earlier this year, 80% said they lacked confidence in their cybersecurity posture and plan to invest more!

Are these cybersecurity investments producing desired returns?

Most likely, no. Even as enterprises continue to invest in tools and assets to build cybersecurity forts around their organizations, the ROI is inconsistent at best, negative at worst.
Cybersecurity investments are driven by a combination of operational, technological, and regulatory factors.

Cybersecurity strategy is reactive

Enterprises make specific investments in response to incidents. Whether it’s an accidental breach or a targeted hack attack, enterprises tighten their boundaries after the fact, by which time it’s too late. This reactive nature of cybersecurity strategy leaves organizations fixing the breakage instead of preventing the fall.

Moreover, given the evolving nature of cybersecurity risks, they end up having to upgrade over and over, making the investment too heavy to see proportionate returns.

Cybersecurity strategy isn’t aligned with organizational goals

Most cybersecurity tools are not devised to be in line with organizational KPIs. Each tool might be set up for specific granular KPIs, but the effectiveness of the overall strategy goes unmonitored.

Tooling and products are chaotic

Enterprises use a wide range of tools, each performing one function. They choose specialized products for firewalls, application security, network security, breach detection, alerting mechanisms, etc. On average, companies deploy 45 tools on their network.

Gaps that expose critical assets

Even when these products are exceptional at what they protect, they don’t speak the same language, so they don’t collaborate well. As a result, the organizational security dashboards see more noise than insights. This creates gaps in coverage, leaving organizations open to breaches.

Compliance demands are evolving

Cybersecurity has regulatory and industry compliance implications. Governments across the globe are slowly building laws and legal protections around online security, data, connectivity, etc. This needs enterprises to continuously develop compliance protocols.

To strengthen the cybersecurity posture and drive better ROI, enterprises need a comprehensive continuous controls monitoring strategy.
Your Cybersecurity booster shot: Continuous Controls Monitoring

A unified single-pane-of-glass solution that continuously monitors, analyzes, and displays your cybersecurity posture by including multiple security frameworks and standards.

Continuous Controls Monitoring (CCM) is a technology solution that automates the continuous monitoring of critical security controls throughout your cybersecurity ecosystem. It performs dynamic scoring of the health and efficiency of your cybersecurity posture, whether on-prem, cloud, or hybrid environments.

Singular intuitive interface

Chief information security officers (CISOs) do not need to navigate multiple complex dashboards to understand the organization’s cybersecurity posture. They can continuously monitor it from a single pane of glass. You can also have ongoing anomaly detection and threat intelligence through continuous polls of various tools.

Business-driven visibility

CCM drives the alignment of cybersecurity strategy with the organization’s technology, business, and regulatory goals. It enables specific and customized views for individual user groups based on critical business assets, empowering teams to adapt on the go.

Dynamic configuration monitoring

You can dynamically verify the configuration of security tools and validate their error-free functioning. You can also retrieve and analyze critical security controls on your tools to enhance risk posture management and facilitate compliance.

Remediation insights

Your technology solutions are interconnected, so are your cybersecurity risks. CCM presents a collaborative opportunity across your entire landscape of tools to identify actionable remediation insights.

Compliance and predictive security

CCM offers an end-to-end view of all compliance requirements, including international standards such as GDPR, HIPAA, PCI, etc. The risk scoring functionality offers predictive capabilities to always stay ahead of threats.
How Continuous Controls Monitoring can transform your enterprise

The fundamental value of a continuous controls monitoring system is optimizing cybersecurity ROI. It does so by:

Enabling end-to-end visibility: From user devices, network, and application to end-point, CCM offers holistic yet granular visibility. This ensures that any gaps or loopholes are identified before they’re breached.

Integrating seamlessly: With support for various security frameworks and 5000+ out-of-the-box critical security controls, CCM integrates into your enterprise tech stack without expensive customizations.

Offers C-level view: Cybersecurity is now a board-level concern. CCM provides a customized business scorecard for every leader, with information that can impact the organization’s value at their fingertips.

Reduces business losses: It ensures robust cybersecurity and compliance posture, predicts potential loopholes, alerts anomalies earlier, and minimizes losses.

Improved ROI: Improve the return on cybersecurity spends, and lower the cost incurred on an attack by identifying and addressing potential threats at its earliest stage.

Cyber observer+  Marlabs to optimize your Cybersecurity ROI

Marlabs brings the strengths of Cyber Observer to power your continuous controls monitoring strategy. Our experts build your strategy, identify critical KPIs, integrate the solution, and set up dashboards for your needs.

To see CCM in action, speak to a Marlabs consultant today.
About Marlabs

Marlabs designs and develops advanced digital solutions that help its clients improve business outcomes swiftly and precisely. It succeeds by harnessing the power of the Digital Collective™, which brings together design-led digital innovation with human experience, composable digital platforms, and a collaborative ecosystem of first-class technology partners and innovators.

Marlabs is headquartered in New Jersey, with offices in the US, Germany, Brazil and India. Its 2500+ global workforce includes highly experienced technology, platform, and industry specialists from the world’s leading technical universities.

Marlabs Inc.(Global Headquarters) One Corporate Place South, 3rd Floor, Piscataway, NJ - 08854-6116, Tel: +1 (732) 694 1000 Fax: +1 (732) 465 0100, Email: contact@marlabs.com

Visit us online at www.marlabs.com