Cybersecurity: Why ROI isn't always a meaningful metric

BY ANNA HAMMOND · JUNE 4, 2024 · LAST UPDATED ON MARCH 6, 2025

Cybersecurity investments are crucial for businesses of all sizes, but determining the return on investment (ROI) of these investments can be complex. Conventional ROI methodologies often fail to encompass the complete value of cybersecurity measures, resulting in a distorted view of their efficacy.

Are you seeking an effective way to communicate the significance of cybersecurity to your board and gain their support for vital security measures? In this article, we'll explore whether ROI provides a comprehensive evaluation of cybersecurity posture.

The problems with ROI

The exclusive reliance on ROI as a yardstick for cybersecurity investments is not without its problems. Although ROI is a valuable financial measure for assessing investment profitability, it doesn't fully gauge the value of cybersecurity. Focusing solely on financial returns when making cybersecurity investments, for example, overlooks the broader implications these investments have on an organization's overall security posture and its ability to withstand long-term cyber threats.

Here are some key limitations of using ROI as a metric in cybersecurity:

ROI is a backward-looking metric

ROI measures the profitability of an investment that has already been made. However, it doesn't provide any insights into the potential future value of an investment. Cybersecurity investments often have a long-term impact, and their benefits may not be immediately realized. For example, a cybersecurity investment that prevents a data breach may not generate any immediate financial returns. However, in the long run, it can save the organization millions of dollars by avoiding breach-related costs such as fines, legal fees, and customer loss.

ROI doesn't accurately reflect the value of cybersecurity investment

ROI is often calculated using financial metrics, such as profits and losses, which may not accurately reflect the value of cybersecurity investments. Cybersecurity investments often yield benefits that are challenging to quantify in financial terms, such as enhanced brand reputation, heightened customer trust, and mitigated operational risks. These benefits can significantly impact an organization's overall success, yet they may not be captured in conventional ROI calculations.

Cybersecurity prevention is difficult to assign monetary value to

The returns from cybersecurity investments are often intangible and challenging to quantify, presenting a conundrum in accurately calculating the ROI. For example, how does one assign a monetary value to the

prevention of a data breach?

ROI does not consider the risk of cybersecurity incidents

While a cybersecurity investment may indeed yield a high ROI, the risk must be carefully assessed. If the investment does not provide adequate protection from cyber threats, the potential cost of an attack could eclipse the benefits of the investment. For example, a new firewall may boast a high ROI, but if it fails to defend against a sophisticated cyberattack, the costs could be substantial.

Difficulties gathering data at scale to measure ROI

One of the primary challenges in calculating ROI for cybersecurity investments is the difficulty of gathering comprehensive data at scale. Cybersecurity data is vast and varied, encompassing everything from incident reports and breach costs to less tangible metrics like employee awareness. For large organizations, this data is spread across multiple departments and systems, making it difficult to aggregate and analyze effectively. The sheer volume of data, coupled with its sensitive nature, requires robust data management and analysis tools, which can be a significant hurdle for many organizations.

The changing nature of the industry makes calculating ROI challenging

The cybersecurity industry is characterized by rapid technological advancements and an ever-evolving threat landscape. New vulnerabilities and attack vectors emerge regularly, requiring constant updates to security protocols and measures. This dynamic nature makes it challenging to maintain a consistent and long-term ROI calculation as the effectiveness of security investments can fluctuate based on the current threat environment.

Additionally, the regulatory landscape is also changing, with new laws and standards frequently introduced, impacting how organizations manage their cybersecurity strategies and investments. Consider the UK's **Product Security and Telecommunications Infrastructure (PSTI) Act**, for example. As of April 2024, the regulation required those impacted to follow specific security standards and protocols. One new requirement was clear guidance on how to report security concerns regarding their product. For many, this meant setting up a **vulnerability disclosure program**.

What is a vulnerability disclosure program

Why ROI might be misleading

Relying solely on ROI to evaluate cybersecurity investments can be misleading and hinder effective decision-making. A significant challenge in evaluating cybersecurity investments is quantifying their benefits. Unlike tangible assets or revenue-generating projects, cybersecurity investments often yield intangible benefits. Examples include risk reduction, enhanced brand reputation, and increased customer trust. Assigning precise monetary values to such qualitative factors is complex and subjective.

Furthermore, the absence of direct counterparts in other domains complicates ROI assessments. For example, comparing the ROI of a cybersecurity initiative to that of a marketing campaign or a new product development project is challenging due to the lack of standard benchmarks. This can lead to ROI calculations that are not only difficult but also potentially misleading.

Finally, cybersecurity investments are known to have long payback periods. The benefits of these investments may not be realized for many years, rendering short-term ROI calculations less meaningful. This can present challenges when seeking funding for cybersecurity initiatives, especially when compared to projects with more immediate returns.

When can ROI be a useful metric in cybersecurity?

While ROI has several limitations as a metric for cybersecurity investments, there are certain scenarios where it can provide valuable insights. Here are a few situations where ROI *can* be a useful metric:

The business has well-defined cybersecurity risks

When an organization has a clear grasp of the cybersecurity risks it faces, and these risks can be quantified, ROI can be a valuable tool for evaluating the effectiveness of cybersecurity investments. By weighing potential losses from security incidents against the costs of security investments, organizations can make informed decisions about the value of their investments.

There are easily measurable benefits

In instances where the benefits of cybersecurity investments can be readily quantified and monetized, ROI becomes a more dependable measure. For example, should an investment in cybersecurity prevent a data breach that would have led to financial losses, the ROI can again be seen by comparing the investment cost with the averted losses.

Small investments with high potential returns

ROI can be a valuable tool when assessing smaller cybersecurity investments that have the potential for a high return. Here, the payback period is brief and the investment's associated uncertainty is diminished. Therefore, ROI is a more dependable gauge of the investment's worth.

Alignment with strategic goals

When cybersecurity investments are aligned with the organization's overall strategic goals, ROI can be a valuable metric to assess their effectiveness. By linking cybersecurity investments to specific business objectives, organizations can evaluate whether these investments contribute to achieving their broader strategic goals.

Alternative ways to evaluate cybersecurity

Organizations are advised to explore alternative metrics for the effective evaluation of cybersecurity investments. Metrics like the cost of avoided security incidents or the number of prevented breaches give clearer insights into the value of these investments. These metrics are more closely aligned with the primary objective of cybersecurity: the protection of sensitive data and critical infrastructure.

Here are 5 alternatives to evaluating cybersecurity:

1. Return on Security Investment (ROSI)

Return on Security Investment (ROSI) is a metric used to assess the efficiency of cybersecurity investments. It calculates the financial value that security measures contribute by reducing the risk and potential costs of security incidents. ROSI helps organizations determine the effectiveness of their security spending by comparing the cost of security implementations against the financial losses prevented. This calculation supports strategic decision-making by highlighting the economic benefits of investing in robust security systems, such as **bug bounty programs**, to maintain operational continuity and protect the organization's reputation.

2. Risk reduction metrics

One of the primary ways to evaluate cybersecurity is through risk reduction metrics, which focus on measuring the decrease in vulnerabilities and security incidents. This approach involves tracking the number of identified vulnerabilities over time, noting how quickly they are addressed, and monitoring the frequency and severity of security incidents. By demonstrating a downward trend in these areas, organizations can quantify how effectively their cybersecurity measures are mitigating risks. This metric is crucial as it directly correlates to the organization's ability to protect its assets and data from potential threats.

3. Cost avoidance

Cost avoidance is another critical metric for evaluating cybersecurity. This includes calculating the costs that have been avoided through proactive security measures. For instance, by implementing advanced security technologies and practices, an organization can avoid costs associated with data breaches, such as legal fees, fines, and remediation costs. Additionally, proactive security can prevent increases in cyber insurance premiums, which often rise following a security breach due to perceived increased risk. Estimating avoided costs can be complex but provides valuable insight into the financial benefits of investing in robust cybersecurity measures.

4. Compliance and standards adherence

Adhering to compliance standards such as the General Data Protection Regulation (GDPR) and the **PSTI Act** is another way to evaluate cybersecurity effectiveness. Compliance metrics assess an organization's ability to meet specific regulatory requirements, which can help avoid penalties and fines associated with non-compliance.

Moreover, maintaining compliance helps in safeguarding sensitive data, thus enhancing an organization's reputation and trustworthiness. Regular audits and assessments can track compliance levels, ensuring that the organization remains aligned with industry standards and regulations.

5. Operational metrics

Operational metrics provide a practical view of the cybersecurity landscape within an organization. Key operational metrics include system uptime, incident response time, and mean time to recovery (MTTR). System uptime measures the reliability and availability of IT services, directly impacting business operations and productivity. Incident response time is critical for minimizing the damage from security breaches, reflecting the efficiency of the response team. MTTR focuses on the speed of recovery from cyber incidents, indicating the resilience of the organization's IT infrastructure. These metrics are

essential for operational planning and can significantly influence strategic decisions regarding resource allocation and cybersecurity investments.

Communicating cybersecurity value to the board and getting buy-in

Communicating the value of cybersecurity to the board of directors and securing their support is critical for achieving cyber resilience. Translating technical jargon into business risks they can understand is key. Illustrate real-life examples of cyberattacks that have caused financial and reputational damage to organizations. Quantify the potential cost savings of investing in cybersecurity. For example, Visma's Bug Bounty Program Manager, Ioana Piroska, gave the following explanation when pitching crowdsourced security to the business: "Our Security Director has a simple rule of thumb. He says $1 spent in bug bounty is between $10 and $100 saved later."

Visma highlights the financial impact of its bug bounty program

Emphasize the role of cybersecurity in protecting the organization's intellectual property and sensitive data. Present a comprehensive cybersecurity risk management plan that outlines strategies for mitigating risks and a clear path forward. By making a compelling case for cybersecurity as a strategic priority, you can gain the board's support and the resources needed to strengthen your organization's security posture.

The financial impact of the crowdsourced security model

Calculating cybersecurity ROI has its challenges. However, crowdsourced security methods offer a compelling solution for security teams looking to maximize their cybersecurity budgets and positively impact the organization's bottom line.

The crowdsourced model allows organizations to extend their cybersecurity capabilities without the need to expand in-house teams. With a global community of security researchers, organizations can continuously test for new vulnerabilities across their digital assets. The community has a wide variety of skills, which helps organizations find and fix security issues more quickly than working alone.

Intigriti has 90,000 ethical hackers signed up to its platform, assisting companies like Microsoft, Dell, BMW, Coca Cola, and Monzo to ensure their attack surface is protected. Ready to outmaneuver cybercriminals with global crowdsourced security? Book a meeting today!