ManageEngine
Log360 MSSP

The cost of cybersecurity: How MSSPs offer economic efficiency

With cyberthreats looming larger and being more sophisticated than ever, cybersecurity is not just a necessity, but a critical investment for businesses of all sizes. However, the cost of maintaining robust cybersecurity can be daunting especially for small and medium-sized businesses (SMBs) and enterprises. It's a significant challenge to strike the right balance between ensuring comprehensive security systems and managing budget constraints. This is where managed security service providers (MSSPs) come into play, offering hope for businesses that are grappling with these concerns.

In this ebook, we will get into the complexities of cybersecurity costs and see how MSSPs provide an economically efficient alternative. We will explore how MSSPs not only enhance security, but also smartly optimize expenses. MSSPs offer businesses a strategic pathway to safeguard their digital assets without breaking the bank.

The cost of cybersecurity: An overview

Cybersecurity costs vary based on multiple factors. As the cyberthreat landscape evolves, businesses must adapt their cybersecurity strategies and investments accordingly, making it an essential and dynamic component of modern business operations. For that, understanding and addressing diverse factors is key to businesses protecting themselves against cyberthreats while managing their cybersecurity investments efficiently. Let us take a look at the factors that determine the overall cybersecurity costs of an organization.

- **Industry-specific vulnerabilities:** Certain industries—such as finance, healthcare, and IT—face higher risks due to the sensitive nature of the data they handle. This necessitates enhanced security measures and subsequently higher cybersecurity costs.

- **Organizational size and employee count:** Larger companies with more employees have increased potential entry points for cyberattacks, as each device and workstation could be exploited. This escalates cybersecurity costs, with industry averages suggesting around $2,000 per employee.

- **Hardware and software infrastructure:** The specific technologies a company uses dictate the type and extent of cybersecurity measures needed. Protecting diverse technology stacks, like servers and websites, requires sophisticated solutions, and increases costs.

- **Security vendors, products, and services:** The choice of cybersecurity vendors and their offerings significantly affects total costs. Opting for more comprehensive protection typically results in higher expenses. Additionally, the decision between self-installation or professional installation of security products can impact the overall budget.

- **Employee training:** Human error is a common cause of breaches and necessitates investment in employee cybersecurity training. Larger organizations might also need to hire dedicated security professionals, adding to the costs.

- **Incident response and recovery:** Dealing with cyberattacks involves costs for mitigation, notification, and preventive measures. Cybersecurity insurance is an added factor that helps cover these expenses.

- **Organizational complexity:** The more complex an organization—in terms of network size, multiple locations, and data volume—the higher the cybersecurity expenses.

- **Compliance requirements:** Different industries have varying levels of regulatory compliance requirements, with sectors like finance and healthcare facing stringent standards. Meeting these regulations necessitates higher investments in cybersecurity.

- **Current IT infrastructure:** The state of a company's existing IT infrastructure also influences costs. Outdated systems often require comprehensive upgrades to meet current security standards. A company's chosen security strategy, whether focusing on advanced technologies, proactive threat detection, or incident response, significantly affects the budget.

MSSP offerings: How you can reduce your cybersecurity costs

The outlined complexities and varied costs associated with maintaining cybersecurity in-house clearly indicate that a streamlined and cost-effective approach is desirable. This is where the value of MSSPs are apparent. MSSPs offer a tailored solution that addresses the multifaceted challenges of cybersecurity costs, turning what can be a significant business burden into an efficient, managed service. In the following section, we will cover the specific ways MSSPs can significantly reduce cybersecurity costs for organizations. By exploring the economic benefits of MSSP offerings, we will see how these services not only enhance security but also optimize financial investments in cybersecurity.

Here are the key economic advantages of partnering with an MSSP:

- **Reduction in direct cybersecurity expenses:** MSSPs help businesses avoid the substantial investments required in building an internal cybersecurity team. This solution lowers the financial burden for each business by spreading the costs of advanced security solutions and continous monitoring across multiple clients. This includes savings on hiring, training, and equipping a dedicated cybersecurity staff.

- **Access to expertise and advanced technology:** Partnering with an MSSP provides businesses with access to state-of-the-art technology and a team of specialists experienced in international cyberthreats. This eliminates the need for individual businesses to invest in expensive cybersecurity infrastructure or specialist staff.

- **Predictable and manageable costs:** Outsourcing cybersecurity to a MSSP replaces unpredictable expenses with a consistent and manageable monthly fee. This aids in effective budgeting and financial planning for businesses, ensuring no surprise costs.

- **Prevention of costly data breaches:** MSSPs offer sophisticated cybersecurity measures that significantly reduce the risk of data breaches. This preemptive approach is critical considering the high costs associated with data breaches. For instance, major incidents like the Sony data breach have cost companies millions of dollars in damages, investigation costs, IT repairs, lost profits, and litigations.

- **Efficient resource allocation:** Companies can redirect resources that would have been spent on cybersecurity towards core business functions, thus improving overall efficiency and productivity. This strategic allocation of resources contributes to business growth and stability.

- **Return on investment (ROI):** Studies by CompTIA have shown that businesses utilizing MSSP services achieve significant cost reductions. To be exact, 46% of businesses using managed IT services reported reducing their annual IT costs by at least 25%.
- **Reduction in hardware:** MSSPs typically employ a SaaS model and manage their own hardware, which reduces the need for businesses to invest in technology infrastructure.
- **Stable and no unexpected expenses:** Partnering with an MSSP provides financial clarity with stable, consistent expenses. MSSPs manage compliance, vulnerability assessments, and routine scans, eliminating surprise expenses for businesses. They stay up-to-date with the latest regulations and guidelines, ensuring that clients' systems are always in compliance and protected against emerging threats.
- **Employee cost savings:** Without the need for an in-house security team, businesses can save a considerable amount on employee-related costs. These savings extend beyond salaries to include facilities, benefits, and other compensation expenses. MSSPs remove the need for costly recruitment processes and staff training in cybersecurity.

Choosing the right solution for you

The adoption of an MSSP partnership offers a transformative approach for businesses navigating the complex and often costly landscape of cybersecurity. The economic advantages of MSSPs are clear: From significant reductions in direct cybersecurity expenses to the provision of state-of-the-art technological resources and expertise. By partnering with an MSSP, businesses can not only anticipate a more predictable and manageable cost structure, but also strengthen their defenses against the evolving cyber threats.

However, an important point that the key to reaping all these benefits also lies in choosing the right MSSP providers. A suitable MSSP aligns with your business' specific needs, industry requirements, and offers tailored solutions that effectively address the unique challenges you face. A well-chosen MSSP becomes an extension of the organization, contributing not just to the safeguarding of its digital assets, but also to its overall operational efficiency, stability, and success.

Our Products

EventLog Analyzer MSSP | AD Manager Plus MSSP

ManageEngine
Log360 MSSP

Log360 MSSP is a unified SIEM solution for MSSPs that helps monitor, manage and secure clients' environments. With client-specific customization and data isolation, Log360 MSSP helps MSSPs handle multiple clients of various sizes. The solution's threat detection and compliance reporting capabilities help MSSPs create value for their clients. For more information about Log360 MSSP, visit https://www.manageengine.com/siem-mssp/

$ Get Quote   ↓ Download