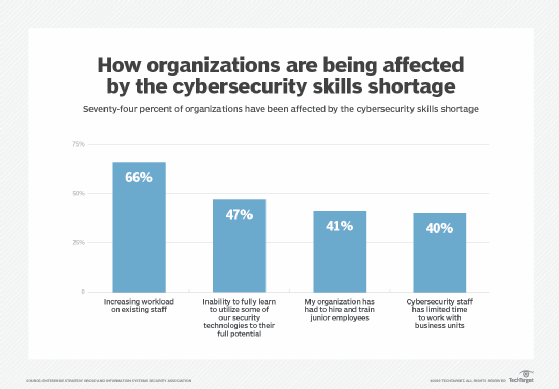
# **How Much Does it Cost to Outsource Cybersecurity**

Cyber security has become a paramount concern in an age where digitalization rapidly transforms businesses' operations. Organizations across the globe are investing heavily in securing their digital infrastructure against cyber criminals but often face the daunting question: "Should we outsource cybersecurity or build an in-house team?"



[Source](https://cdn.ttgtmedia.com/rms/onlineimages/security-cybersecurity_skills_shortage_01_mobile.png)

This article will explore the costs of outsourcing cyber security solutions and services, why companies should consider them, factors impacting the price, and the average expenses. We will also directly compare outsourcing and building an in-house team and outline the essential factors to consider when choosing the right cybersecurity service provider.

## **Why Should Companies Outsource Cybersecurity?**

****

[Source](https://nexttechnology.io/app/uploads/2022/06/OUTSOURCING-CYBERSECURITY-1024x535.jpg)

There are many factors that you should consider why your company should outsource these services, and below are some of them:

### **Access to Specialized Expertise**

Outsourcing cyber security enables many organizations to tap into a pool of experts with specialized knowledge and experience handling diverse cyber threats. These security experts possess threat intelligence, response, security practices, and mitigation skills, often exceeding those of in-house staff.

### **Scalability and Flexibility**

Companies can scale their cyber security needs up or down, depending on their requirements. Outsourcing allows organizations to respond to changing cyber crime landscapes and evolving business needs more effectively.

### **Cost-effectiveness**

Building and maintaining an in-house cybersecurity IT team can be expensive.

Outsourcing allows organizations and business leaders to optimize their budgets by only paying for the services they need while will allow them to save money instead of incurring the fixed costs associated with hiring, training, and retaining full-time employees.

### **Regulatory Compliance and Requirements**

Many industries are subject to stringent compliance and regulatory standards. Outsourcing to a reputable cybersecurity service provider ensures adherence to these requirements, as these providers are well-versed in the latest regulations.

### **24/7 Monitoring Security Team and Support**

Outsourced cyber security providers often offer round-the-clock monitoring and support, ensuring that a cyber attack or suspicious activity is detected and addressed promptly. This level of vigilance can be challenging to achieve with an internal team, especially for smaller businesses with limited resources.

When you completely outsource cyber security services, you can rest assured that they will provide you with security tools such as malware protection programs and other security hardware responsible for protecting data.

## **What Impacts the Cost of Outsourcing Cybersecurity?**

Several factors influence the cost of outsourcing cybersecurity services:

### **Scope of Services**

The range of services required will significantly impact the cost. For instance, a basic monitoring and alert service will cost less than a comprehensive solution that includes potential risk detection, incident response, and ongoing vulnerability management.

### **Company Size and Complexity**

Larger organizations with more complex digital infrastructures will likely incur higher costs due to the increased effort required to secure their systems, as sometimes, you may need to install security standards per user or, sometimes, whenever they use multiple devices if they are working remotely.

### **Industry and Compliance Requirements**

Companies operating in highly regulated industries, such as finance or healthcare, may have to spend more on cybersecurity services to ensure compliance with industry-specific regulations. Sometimes, they are required to have a security operations center.

### **Location and Service Provider**

Costs may also vary depending on the service provider's location and the organization itself. Some regions may have lower labor costs, leading to more affordable services. However, it's crucial to consider the services' quality and not base the decision solely on cost.

## **Average Costs to Outsource Cybersecurity Services**

The cost of outsourcing cybersecurity services can vary widely, depending on the factors mentioned earlier.

### **Small businesses**

Small businesses typically have fewer resources and a less complex digital infrastructure, which results in lower costs for outsourcing cybersecurity. The expenses for small businesses can range from $1250 to $2,500 per month, depending on the scope of services required.

### **Mid-sized businesses**

Mid-sized businesses often have more complex IT environments and higher security requirements, leading to increased costs for outsourcing cybersecurity. For these companies, costs can range from [$3,500 upwards](https://www.accentonit.com/blog/managed-cyber-security-services-cost#how-much-managed-cyber-security-cost), depending on the services and expertise needed.

### **Large companies**

Large companies generally have the most complex IT infrastructures and face more significant security threats due to their size and prominence. Outsourcing cybersecurity for these organizations can be pretty costly, with expenses starting at [$36,000](https://www.scarlettcybersecurity.com/how-much-does-cybersecurity-cost) and going up from there, depending on the range of services and expertise needed.

## **Outsourcing Cyber Security vs. Building an In-House Team - Direct Comparison**

In this section, we will provide a direct comparison between outsourcing cybersecurity services and building an in-house team in terms of initial setup costs, ongoing expenses, and total cost of ownership.

### **Initial Setup Costs**

#### **Outsourcing Cyber Security Services**

In outsourcing cybersecurity services, companies usually experience lower initial setup costs compared to establishing an in-house cybersecurity team. The expenses associated with the initial setup of outsourced services can encompass elements such as the service agreement, procurement of any necessary hardware or software components, and fees related to onboarding.

Despite these costs, they tend to be more budget-friendly overall, primarily because the service provider will likely already have the requisite infrastructure and know-how. This existing foundation not only streamlines the setup process but also ensures that the costs associated with establishing cybersecurity defenses remain manageable and economical, particularly compared to the often higher expenses involved in creating an in-house cybersecurity team from scratch.

#### **In-house**

Creating an in-house cybersecurity team entails considerable upfront expenses encompassing a wide range of aspects. Among these are recruiting and onboarding skilled professionals, investing in their training and development, acquiring the necessary hardware and software tools, and establishing secure environments to implement cybersecurity measures effectively. The financial burden of these initial expenditures can be notably high, particularly for small and mid-sized businesses that may have constrained resources.

Consequently, establishing a strong and dedicated in-house cybersecurity team can be particularly daunting for organizations with limited budgets, as they must balance their security needs with the substantial investment required to put such a team in place.

### **Ongoing Expenses:**

#### **Outsourcing Cyber Security Services**

The recurrent costs associated with outsourcing cybersecurity services comprise the monthly or annual charges levied by the service provider. These fees encompass a variety of services, such as continuous monitoring, detecting and responding to potential threats, and any other agreed-upon services tailored to the organization's specific needs. One of the advantages of these expenses is their predictability, which enables businesses to manage their budgets more and allocate resources accordingly.

Moreover, outsourcing cybersecurity services often gives organizations the opportunity to tap into a greater depth of expertise and knowledge in the field, which might be challenging to achieve with an in-house team. This advantage can be particularly significant when considering that outsourcing often delivers access to top-tier professionals at a comparatively lower cost than the expenses incurred in recruiting, training, and retaining an equivalent in-house team.

#### **In-house**

When maintaining an in-house cybersecurity team, organizations face ongoing expenses that encompass a variety of aspects, such as employee salaries, benefits packages, professional development, and training, as well as the upkeep and maintenance of essential equipment. These costs have the potential to be not only substantial but also unpredictable, given that businesses need to make ongoing investments to ensure that their cybersecurity staff stays abreast of the latest developments in the field. This includes addressing the ever-changing landscape of cybersecurity threats, which demands constant vigilance and adaptation to new challenges.

In addition to the financial implications, in-house cybersecurity teams may necessitate a greater allocation of resources to provide comprehensive, 24/7 monitoring and support. This level of commitment can strain an organization's available resources, especially when considering the need to maintain a highly skilled workforce that can respond effectively to the dynamic nature of cybersecurity threats. Consequently, managing an in-house cybersecurity team often entails a significant investment in both financial and human resources, which can prove challenging for organizations as they strive to balance security needs with other operational priorities.

### **Total Cost of Ownership:**

#### **Outsourcing**

The total cost of ownership when outsourcing cybersecurity services encompasses several financial components, such as the initial setup expenses, the recurring costs associated with maintaining the service, and any supplementary charges that may arise in relation to incident response or the provision of additional services beyond the original agreement. In a significant number of instances, opting for an outsourced cybersecurity solution results in a lower overall cost of ownership when compared to the alternative of establishing and managing an in-house team.

This cost advantage is primarily due to the flexibility and scalability that outsourcing offers to businesses, enabling them to tailor the services they receive to align with their specific security requirements. As a result, organizations only pay for the cybersecurity solutions they genuinely need, avoiding any unnecessary expenditure on resources that may not be relevant to their particular circumstances. This streamlined approach to cybersecurity management ensures that companies can maintain a robust security posture while optimizing their financial investments in this critical area.

#### **In-house**

The all-encompassing cost of ownership for an in-house cybersecurity team considers several crucial financial elements, such as the initial investment needed to establish the team, the ongoing expenses for sustaining its operations, and the potential monetary impact of addressing security breaches or incidents that could arise. Often, the overall cost of ownership associated with an in-house cybersecurity team is higher when compared to outsourcing these services to specialized external providers.

Nonetheless, some businesses might lean towards the in-house option due to its perceived advantages. One such advantage involves retaining direct control over every facet of their cybersecurity operations, ensuring that security measures and protocols are closely tailored to the organization's unique needs and objectives. Moreover, a dedicated in-house team's focus on the company allows for a more targeted approach to security, as team members can cultivate a deeper understanding of the specific risks and challenges that the organization encounters.

## **Choosing the Right Cyber Security Services Provider**

### **Experience and Expertise**

Evaluate the provider's track record and the expertise of their team members. Choosing a provider with extensive experience in the industry and the necessary skills to handle your organization's unique security needs is essential.

### **Range of Services**

Determine if the provider offers a comprehensive suite of services that cater to your organization's requirements. This may include threat detection and response, vulnerability management, compliance management, and employee training.

### **Responsiveness and Support**

Assess the provider's responsiveness and availability for support. It is crucial to choose a provider that can respond to incidents quickly and provide timely support to minimize potential damages.

### **Compliance and Certifications**

Ensure that the provider adheres to industry-specific compliance requirements and holds relevant certifications, such as ISO 27001, SOC 2, or PCI DSS.

### **Communication and Transparency**

Effective communication is vital for a successful partnership with a cybersecurity provider. Choose a provider that prioritizes open, transparent communication and keeps your organization informed about potential threats and ongoing security efforts.

### **Scalability and Flexibility**

As your business grows, your cybersecurity needs may change. Select a provider that can scale its services to accommodate your organization's evolving requirements.

### **Reputation and References**

Research the provider's reputation and request references from existing clients. This will give you an idea of the provider's performance and reliability.

## **To Sum It Up**

The decision to outsource cyber security or build an in-house team is a critical one for organizations in the digital era. Outsourcing offers several benefits, including cost-effectiveness, access to specialized expertise, scalability, and flexibility. While the cost of outsourcing can vary based on several factors, it is generally a more cost-effective solution for many businesses compared to building and maintaining an in-house team.

When selecting cyber security outsourced services, organizations should consider factors such as experience, range of services, responsiveness, compliance, communication, scalability, and reputation. By carefully evaluating potential providers and choosing the right one, companies can protect their digital assets, adhere to regulatory requirements, and focus on their core business functions, ultimately driving growth and success.