

BearingPoint®

A quick guide to IT security outsourcing



BearingPoint®

A quick guide to IT security outsourcing

Why should you outsource your Security Operations Center (SOC)?

Nowadays, most people understand the importance of data and its impact on our daily lives. Several recent political and economic scandals have convinced the last sceptics. Moreover, the GDPR release outlines the responsibilities and accountability of the entities involved in collecting, storing, and processing personal data. In addition to compromising a company's reputation, The leak of personal data leads to substantial financial penalties.

On the other hand, the acceleration of systems interconnections brings new business possibilities while leading to a tenfold increase of the complexity of guaranteeing security. Therefore, ensuring the confidentiality, integrity, and availability of the modern information technology enterprise is a considerable challenge. This statement should continue to hold with the ramp-up of technologies such as the Internet of Things (IoT) or, to be more accurate, the Internet of Everything (IoE).

A company wishing to ensure a sufficient level of security must cover several aspects, including staff education and the development of a robust system. Depending on its level of exposure and risk tolerance, the company may need to set up a cybersecurity operations center. The cybersecurity operations center (CSOC or SOC) has the responsibility to defend against unauthorised activity within computer networks, including prevention, monitoring, detection, analysis, and services restoration.

To successfully achieve this goal, the SOC must be based on the following four pillars.

1. **Business alignment:** Significant business assets should have priority in the SOC strategy.
2. **People:** Continuity, skills, and the retention of key employees should be ensured.
3. **Process:** Well documented tasks and workflows should be established for repeatability, consistency, and efficiency
4. **Technology:** The selection of solutions to analyse security events and response should be appropriate

Based on these four pillars, a SOC could be built on different models, and within this article, we will take you through them. We will, in the end, provide best practices to outsource your SOC successfully. SOC outsourcing is on the rise in several organizations and provides answers to the questions raised when implementing a SOC.

SOC implementation options

The selection of the appropriate SOC model is the cornerstone of every successful cybersecurity strategy. This highly important decision should be discussed at an executive level and consider several aspects such as budget and regulatory requirements, business orientation, and risk tolerance. An excellent approach to cover those aspects is to perform a risk assessment. This analysis should identify the critical business assets and align SOC performance with the business objectives. Following this analysis, the company can consider the different possibilities offered. This offering could be summed up in 3 options hereafter described.

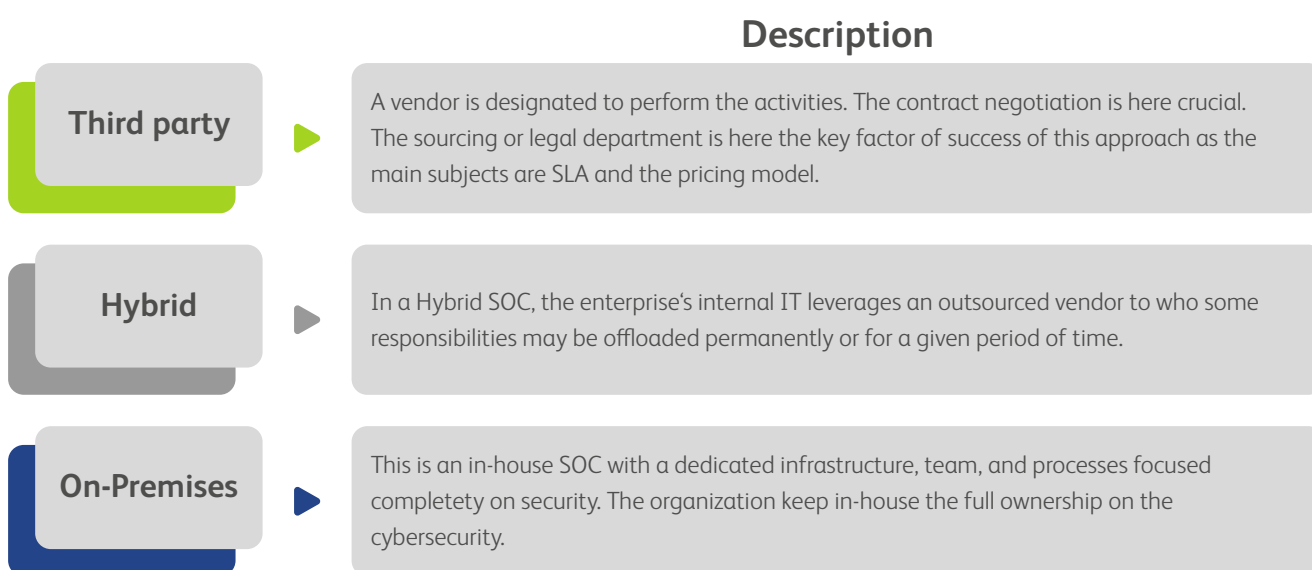


Figure 1: SOC Implementation Models

Building an on-premises SOC

The main advantages provided by this approach are to maintain in-house ownership and control of the SOC. Organizations can then develop internal capabilities and control their security processes. An on-premises SOC allows organizations to adapt their response to the nature of the threats they most commonly face. Using this approach also ensures the in-house retention of all data and de facto helps to stay compliant. Finally, the on-premises SOC allows companies to customize all their systems and applications completely but require a high level of expertise in a variety of technologies. This is the preferred option for an organization with extreme threat exposure in a highly regulated sector.

What are the challenges faced by an on-premises SOC?

Despite the increasing efficiency of tools that assist in organizing, gathering, and analyzing massive amounts of data, having experts on staff is still required to interpret the different sources and information, provide the appropriate assessment, and perform threat remediation. Hiring qualified resources is a real challenge for companies and has led to **a bidding war to attract top talent**. Several reasons could explain why we are facing this situation. The first one is the tremendous increase in demand; nowadays, interconnected systems are ubiquitous, and cybersecurity is a chief concern. Domains such as medical devices, cars and political campaigns need cybersecurity suddenly. In addition, the growing users' concerns about data privacy is forcing companies to improve cybersecurity in order to not jeopardize their reputation. Also, the release of GDPR was a significant shift in the game. It is crucial to understand that a data leak can now lead to substantial financial penalties.

Unfortunately, as useful as the SOC is to the bottom line, it is also a source of significant business costs. As it is not directly profitable for the company, having a SOC will always be a lower priority than core business and commercial activities. Finding a **budget** to finance the SOC is a recurring issue and will continue to be in the future.

Another common issue that several SOCS have is the **lack of documented processes**. The SOC is therefore reliant on individuals' team members' knowledge. This results in an uneven quality of service if the turnover rate is high.

Outsource the SOC to a third party

With this approach, the organization delegates security responsibilities to a third party. The organization only needs to focus on the price for the service and whether the outsourced vendor meets the service level agreements (SLAs).

Several barriers have hindered the progress of this approach. Among those barriers, some companies could find reluctance to share sensitive data. The vendor will unavoidably receive raw data for monitoring and analysis. A leak of this information could drastically increase the risk exposure of the company. Another obstacle is regulations considerations; companies, according to their sectors and countries, are subject to different regulations. An organization outsourcing the SOC must stay accountable and guarantee that data management is compliant with regards to the regulatory context.

Why is IT security outsourcing becoming a top priority?

To handle a growing number of threats and attacks within a more complex regulatory context and amidst growing concerns regarding data privacy (i.e. GDPR) and the challenges faced by an on-premises model, one of the answers is for a majority of IT department to outsource IT Security. Several factors are encouraging this trend, the greatest of which is service vendors' willingness to go downmarket with scalable offerings.

Percentage of organizations increasing amount of work outsourced, by funktion

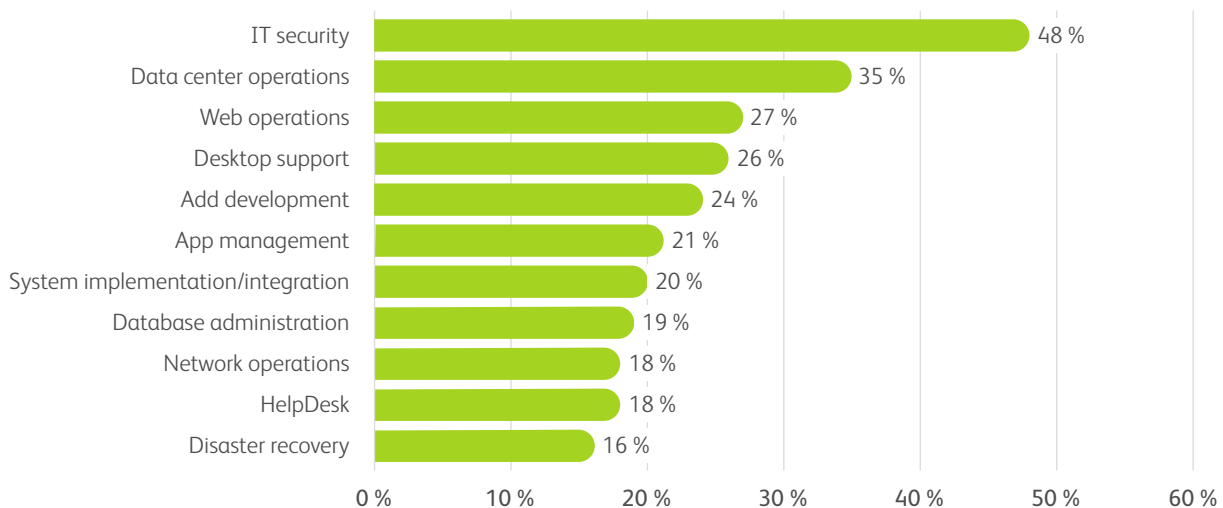


Figure 2: Outsourced security work data, Source: Computer Economics 2019/2020

The main benefits expected by the company outsourcing the SOC's activities are:

- 1. Decrease in the costs of retaining talented experts:**
 By not implementing a SOC on-premises, the company avoid chasing qualified experts to build an efficient team that could solve all SIEM /SOC-related problems. This cost could be very high, as efficient team building could lead to hiring several highly qualified employees.

“55 percent of Organizations considers IT Security outsourcing as a cost-success”
 Source: Computer Economics 2019/2020

- 2. Access to the expertise on demand:** As the threat environment changes continuously, a SOC requires qualified personnel and up to date skills in order to be efficient. The costs of maintaining an SOC operation and of training staff to do so can be prohibitive. A vendor with cybersecurity as a core business and committed to meeting SLA is more willing to hire qualified staff. It is a key asset and more profitable from a business perspective.
- 3. Flexibility and Scalability:** The flexibility enables businesses to respond to the changing requirements. Vendors are expected to adjust services and processes to align with their client's business needs.

Is the hybrid SOC really the best of both worlds?

This option is a combination of the two approaches mentioned above. The organization using a hybrid SOC can keep in-house manage security during regular working hours and utilize a managed service outside of normal working hours, guaranteeing service round the clock.

Another way to use this model is to combine in-house engineers and the Managed Security Service Provider's (MSSP) expertise to create a single operations center. The scope of the security center is shared between the in-house team and the external partner.

The constraint implied by this approach is to have transparent governance to manage the interactions between both teams. Good coordination is the key to get the most out of this model. Some issues need to be addressed, such as the technologies to use and responsibilities. It may look simple, but it could be challenging to define each team's scope and limit. The hybrid model suits organizations that will never fully outsource their entire security capability but are willing to access the expertise and monitoring capabilities that could offer an MSSP (Managed Security Service Provider).

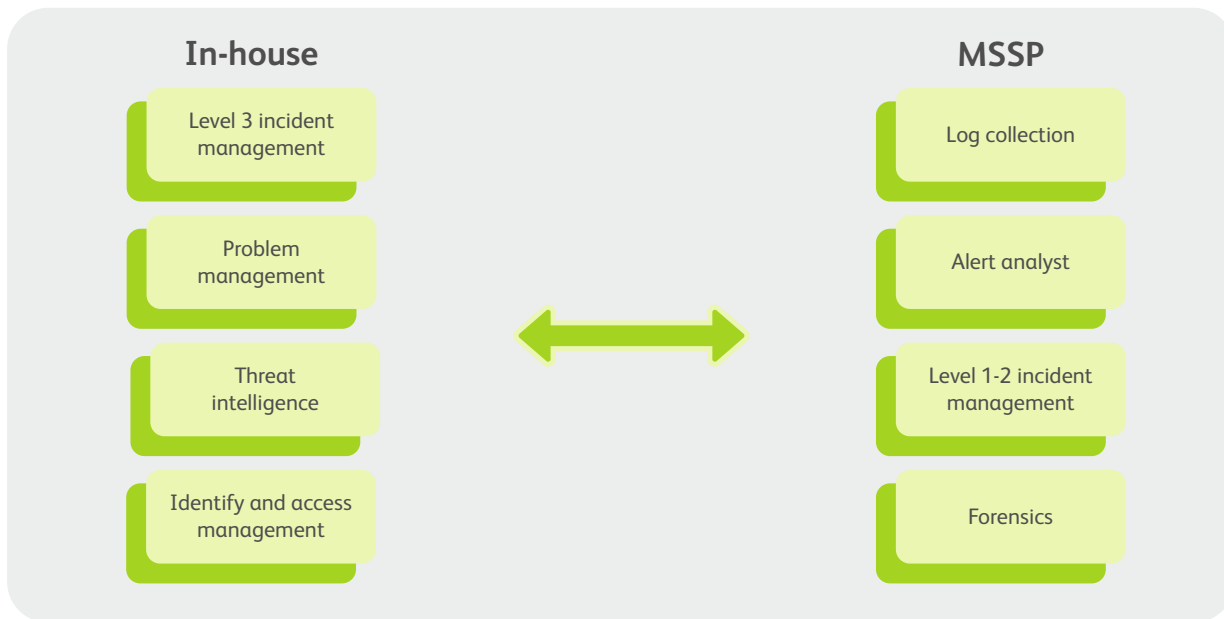


Figure 3: Example of a hybrid model

What are the best practices to successfully outsource your SOC?

The reluctance of some organizations to outsource security due to regulatory considerations or a willingness to preserve critical data access are legitimate. However, professionalism and knowledge of the best practices help contain those risks appropriately.

Here are the fundamental principles to follow to expect a successful SOC outsourcing.

- Review the last Risk assessment for accuracy; some processes or situations are lacking in that area, conduct a rigorous RISK assessment: Any organization should have a clear understanding of its risk tolerance, the threats environment as well as regulatory constraints. This step will also clearly answer the question of how effective the current operations are.
- Clearly articulate the requirements to the vendor. The Risk assessment is a valuable input to write the RFP. The RFP requirements should clearly emphasize the organization's specific needs in data retention, data privacy, regulations, etc.
- Engage the vendor in a continuous improvement process to optimize the threat handling processes. The automation of the process should be considered and lead to cost savings in the long run.

- Regularly conduct proper due diligence on third-party vendors to collect evidence on the services performed.
- Engage the vendor to assist and train you to provide all the evidence requested in case of a compliance assessment. Outsourcing does not exempt you from accountability. You must be able to provide all relevant documentation in case of an audit; you cannot just point at your vendor.

Choose the right partner for outsourcing your SOC!

Deciding to outsource SOC functions partially or entirely is a significant decision. Choosing the right way to implement an enterprise SOC is a critical decision. A misjudgment of the threat environment or the organization's actual capabilities will lead to an inoperable and ineffective SOC. The organization will therefore be exposed, and vulnerabilities will be exploited with potentially significant consequences. This decision must be taken objectively, and the contribution of a completely independent partner can be a considerable asset. BearingPoint's market knowledge and proven experience in sourcing enable our clients to take advantage of best practices. We are covering the whole sourcing lifecycle from strategy to its implementation. Our well-proven tools and methodologies will help you achieve your outsourcing successfully.

About BearingPoint

BearingPoint is an independent management and technology consultancy with European roots and a global reach. The company operates in three business units: The first unit covers the advisory business with a clear focus on five key areas to drive growth across all regions. The second unit provides IP-driven managed services beyond SaaS and offers business critical services to its clients supporting their business success. The third unit provides the software for successful digital transformation and regulatory requirements. It is also designed to explore innovative business models with clients and partners by driving the financing and development of start-ups and leveraging ecosystems. BearingPoint's clients include many of the world's leading companies and organizations. The firm has a global consulting network with more than 10,000 people and supports clients in over 75 countries, engaging with them to achieve measurable and sustainable success.

For more information, please visit: www.bearingpoint.com

Contact



Thorsten Vogel
Partner
thorsten.vogel@bearingpoint.com



Wilfried Fritz
Senior Manager
wilfried.fritz@bearingpoint.com

Authors: Moustapha Chetima, Wilfried Fritz

BearingPoint®