Service-level agreements in cybersecurity: Everything you need to know

BY ANNA HAMMOND · MAY 8, 2024 · LAST UPDATED ON MARCH 6, 2025

To stay on top of relevant and emerging threats, CISOs must adjust and refine their cybersecurity strategies to address the rising challenge of attack surface expansion. As a result, organizations increasingly use service-level agreements (SLAs) to ensure their security providers meet their needs and expectations.

SLAs are contracts that outline the services, metrics, and responsibilities of service providers and customers. Having one in place also ensures remedies or penalties are agreed upon in advance should an SLA not be achieved. In the context of cybersecurity, the agreement is a critical component of any new vendor contract.

In this article, we'll discuss SLAs in cybersecurity, including their key elements, advantages, challenges, and tips for successful management. Here's everything we're going to cover:

What is an SLA in cybersecurity?

An SLA in cybersecurity is an important document that explains the terms and conditions for security services. This includes things like response times to security incidents, protection against cyber threats, and incident resolution procedures.

SLAs clarify the responsibilities of the service provider and the rights of the customer, reducing the chances of conflicts later down the line.

The key elements of a cybersecurity SLA

Now we've covered the basics, let's dive into the key elements that should be included within a cybersecurity SLA.

1. Scope of services

This section clearly defines the specific cybersecurity services that the provider will deliver. It encompasses a comprehensive range of measures, including intrusion detection and prevention, data

encryption, vulnerability assessment and management, and incident response. By outlining these services, both parties have a clear understanding of the protection mechanisms in place.

2. Service level objectives (SLOs) and key performance indicators (KPIs)

SLOs and KPIs are essential for assessing the effectiveness of cybersecurity services. SLOs establish the targeted levels of performance for specific metrics, such as uptime, response time, and successful threat detection. KPIs, on the other hand, monitor and report on the actual performance against these targets. This data-driven approach enables continuous improvement and ensures that the provider meets the customer's security requirements.

3. Roles and responsibilities

Clearly defining the roles and responsibilities of both parties is paramount to ensuring a successful SLA. The SLA should specify the customer's obligations, such as providing accurate and timely information, and the service provider's commitment to delivering services following agreed-upon standards.

4. Data privacy and compliance

In today's data-driven landscape, protecting sensitive information is of utmost importance. The SLA should explain how the service provider will protect the customer's data according to data protection rules and industry standards. It should also outline the procedures for handling data breaches or security incidents, ensuring a prompt and effective response to any potential damages.

5. Service availability and disaster recovery

The SLA should specify the uptime guarantee for cybersecurity services, ensuring minimal disruptions to the customer's operations. It should also detail the response time for resolving incidents and the protocols for backing up and restoring data in the event of a disaster.

6. Termination and remedies

This part of the SLA clarifies the conditions for terminating the agreement for either party. It also outlines the necessary steps to be taken in case of breaches or failure to meet agreed standards.

Intigriti highlights the key elements of a cybersecurity SLA.

The benefits of having a cybersecurity SLA

Implementing a cybersecurity SLA offers many benefits to an organization, including the following key advantages:

Clear expectations and responsibilities

Both the service provider and the customer have pre-agreed responsibilities from the start, which creates accountability for keeping a safe environment.

Well-defined performance metrics

Cybersecurity SLAs supply a structured approach to monitoring and reporting on cybersecurity performance. By defining specific SLOs and KPIs, organizations can identify areas of poor performance and take action to fix them.

Legal and regulatory compliance

Another significant advantage of cybersecurity SLAs is their ability to mitigate risks and ensure compliance with industry regulations and standards. SLAs reduce security breaches and data loss by outlining necessary security measures for organizations to implement. Additionally, SLAs can help organizations in meeting their compliance obligations by ensuring that the cybersecurity services they receive align with relevant laws and regulations.

Cost management

Finally, cybersecurity SLAs serve as a valuable tool for managing costs and optimizing cybersecurity investments. They make sure organizations get the most value for their money by clearly stating the

services and expected performance. This financial transparency and accountability contributes to effective budgeting and resource allocation.

Common challenges in SLA implementation

As the old saying goes, nothing worth having ever comes easy! While SLAs aren't overly complicated, they can come with some challenges.

One common hurdle is ensuring that the SLA aligns with the organization's overall business objectives. Without proper alignment, gaps in protection can arise. To address this, involving key stakeholders from various departments during SLA development is crucial. This collaborative approach helps ensure that the SLA supports the organization's broader strategy.

Another challenge lies in setting up and agreeing on clear performance metrics. If done incorrectly, this can result in choosing metrics that don't accurately reflect the performance of the services. Organizations should collaborate with their cybersecurity providers to establish SMART metrics. This level of clarity will help track performance and identify areas for improvement.

Finally, rapid advancements in technology can quickly make SLA provisions outdated or insufficient for addressing emerging cybersecurity threats. To combat this challenge, it's important to regularly update and review the SLA to incorporate changes in technology and security practices.

Best practices for effective SLA management

To effectively manage a cybersecurity SLA, it's useful to keep the following best practices in mind:

Always include relevant stakeholders

Involve all key stakeholders from both the customer and service provider sides in the SLA development process. This ensures all bases are covered and no information gets left out.

Use clear and precise language

Use precise and understandable language to avoid ambiguity and make sure that all parties have a shared understanding of the terms and conditions.

Regularly review and update the SLA

Regularly review the SLA to keep it up-to-date and relevant, especially in the face of evolving technology and cybersecurity risks.

Be prepared to build some flexibility into the SLA

Integrate flexible clauses to navigate unprecedented changes in technology or organizational demands without compromising the agreement's integrity.

Establish a communication plan

Develop a communication plan that includes regular meetings, status updates, and channels for promptly addressing concerns.

Regularly assess vendor performance

Schedule regular assessments of the service provider's performance against the SLA terms and fix any identified issues.

Final thoughts

Hopefully, this article has helped to clarify the benefits of implementing a cybersecurity SLA. Companies can look forward to increased clarity, more defined metrics, compliance and legal assurances and better cost management. Though some effort is needed to set up and maintain a robust SLA, the dividends it pays in terms of cybersecurity resilience and operational efficiency are well worth the investment!

Keen to get into the nitty gritty of cybersecurity SLAs? Speak to one of our experts to learn more about how Intigriti can support your cybersecurity strategy.