Managed Services Case Study

CISOSHARE
MOVING SECURITY PROGRAMS FORWARD

CISOSHARE Builds and Manages Security Program for a Growing B2B

"Create a balance between the ability to make informed security decisions and the ability to implement them in the shortest timeframe possible. This enables organizations to effectively manage and address vulnerabilities in their program."
– Mike Gentile

Executive Summary

A rapidly growing B2B initially approached CISOSHARE for foundational security program development, which later turned into a longer, continuous managed service contract. After identifying specific processes that the client's internal team didn't have the capacity for, CISOSHARE's managed service team took on these processes to alleviate the need for additional training and resources.

Objective

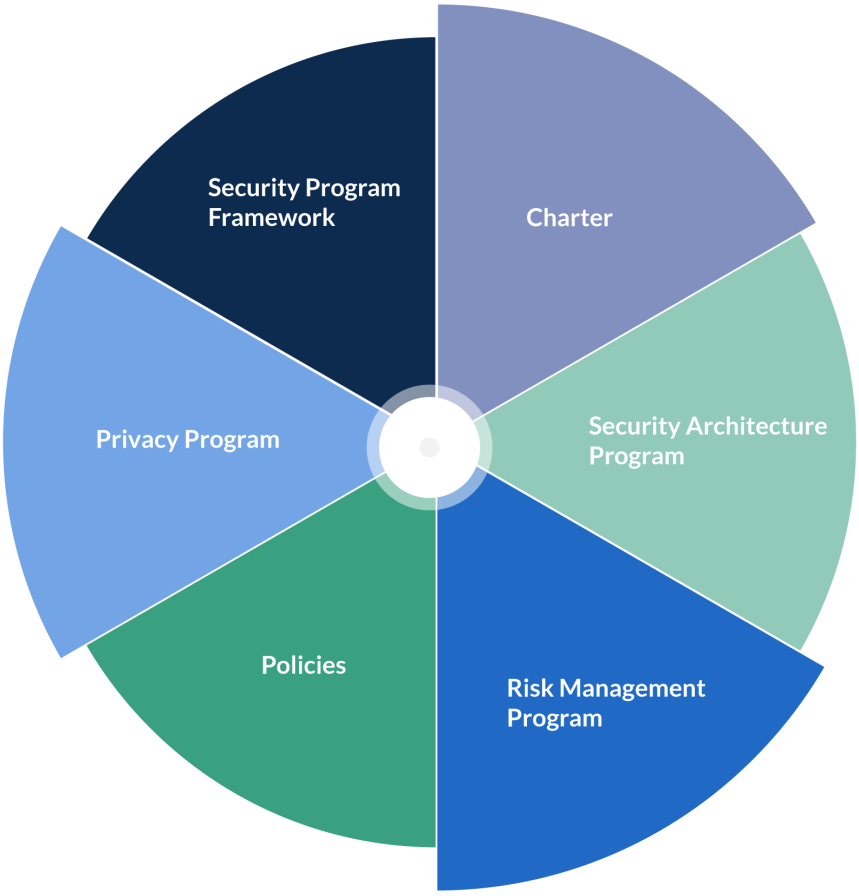
The client's primary objective was to improve their overall security program for the sake of their customers. They identified specific areas for improvement, such as GDPR compliance because of where certain customers were located, as well as the fact that their operations and development teams were based out of Poland. The company also wanted to use security as a differentiator from their competitors, specifically in their preparation for SOC2 Type 2 certification.

Methodology and Process

The CISOSHARE team began this engagement by building the foundations of the organization's security program. The company didn't have accurately defined policies and processes for what the security team was performing, and their program lacked a defined scope. This meant that different tasks were going slowly because a variety of roles would be assigned to tasks without any clear direction.

The CISOSHARE team addressed these issues by focusing on building foundational documentation, including their security program framework, charter, policies, risk management program, security architecture program, privacy program, and other areas that applied to their business needs.

Elements for Building Foundational Documentation



Developing the Framework, Privacy Program, and GDPR Compliance

The team first conducted a demographic analysis of the company to determine the types of information that they store, manage, process, and where they do business. Using this information, we identified best practices and regulatory requirements that the company had to adhere to; in this case, GDPR and PCI. We worked with the company's team to determine whether they wanted strict or flexible compliance with these requirements.

With all the relevant information gathered, our security team created an inventory of requirements for their security program. These requirements come together in a single document to create the security program's framework. From there, the requirements that apply to specific privacy regulations were broken out into the organization's privacy program.

GDPR compliance came hand-in-hand with the privacy program. Complete alignment spanned across legal, compliance, and security. The CISOSHARE team came in to help establish the roles and responsibilities, as well as the scope of how involved the security team would be with GDPR-specific requirements. Our team worked with representatives from legal and compliance to identify which items would be the security team's responsibility.

Managed Process Performance

After establishing the security program's framework and other foundational areas, the CISOSHARE team shifted focus on performing the processes for each of the program areas.

Scheduled processes could include annual pen tests or quarterly vulnerability scans, while **ad-hoc processes** were done as they appeared, such as responding to customer assessments and conducting assessments on third-party partners.

For scheduled processes such as pen tests, the CISOSHARE team supports the internal security team in testing their applications and overall network, both on-premises and in the cloud. Our team verified the vulnerabilities that were picked up by the automated scan to verify accuracy and assigned a ranking for the criticality of the

vulnerability. All the verified vulnerabilities were put into the risk register, and critical or high-priority items were put onto a list to be remediated within fifteen days.

There are specific ad-hoc processes that are assigned to internal roles on the client team, while CISOSHARE provides support with specific processes that don't have a fixed velocity. The number of incoming customer assessments, for example, could change from month to month. By outsourcing this process to our team, the existing security resources on the client team can focus on other, more regular security processes.

Challenges

As previously mentioned, managing the scale and velocity of certain processes — completing customer assessments, for example — was difficult for the client to resource properly. There was no fixed velocity for customer assessments, meaning that one month there could be two assessments to complete, and then fifteen the next, and none in a few months' time.

By identifying processes that were difficult to resource due to inconsistent scale and velocity, the CISOSHARE team was able to assign the process to our own resources and relieve the burden from the client's internal security team.

Another challenge our team faced while establishing the security program was in securing everyone's time in the organization and making sure that employees and management were all on the same page. Our team addressed this by building a clear and accurate scope to utilize each resource's time efficiently.

Because the team focused on building the scope first, this helped the security team understand the responsibilities and which teams would lead which tasks. Having a defined scope and charter made it easier to assign and measure tasks, rather than having to ask multiple people about a given process.

Results

Since CISOSHARE has begun our engagement with the client, a lot of progress has been made with their current security program. The security program is now accurately documented and GDPR-compliant for the sake of where the company conducts business. The security team now has regular meetings with management up to the CEO to provide a more regular flow of information and visibility into the program that didn't exist previously.

After the CISOSHARE team also took on the customer assessment processes, the security team was also able to remediate many of the items that were flagged in previously conducted customer assessments.

The organization is also beginning the process for SOC accreditation. CISOSHARE has provided a dedicated project manager to lead them in their preparation phase, as well as an audit partner to conduct the SOC audit.