

# Professional Services Case Study



**CISOSHARE**  
MOVING SECURITY PROGRAMS FORWARD

## A Symphony of Execution During Major Organizational Changes

*"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

Many security program development efforts encompass a series of dependent projects that need to be performed in a specific order and in the flow of an organizations business. From framework development to building cohesive set of security policies and processes, to the enhancement of a comprehensive security architecture.

Most importantly, these efforts are often required during key times of organizational change. As an organization changes, so must the security program that protects it.

Areas of change in an organization that are common for our customers to want to use our professional services include:

- **Acquisitions:** Being acquired, acquiring others, or selling business units
- **Global Expansion:** Movement of a business into a new global market or demographic
- **Our Customers Demand it:** Needing to be more secure to win or maintain contracts
- **Rapid Growth:** The company isn't a mom and pop shop anymore, and the security program can't be either
- **After the Security Breach:** Having recovered from an attack, it can't happen again
- **Accreditation:** Proving company security through security certification or accreditation
- **Venture/Equity Investment:** Infusion of capital spawning business growth and development
- **Product/Service Expansion:** Entering into new industry with different security requirements
- **Board Invested in Security, Now What?:** Security program investment without results

This document provides a summary of each situation, as well as some of the unique challenges that our team and the organization faced.

## Program Development During a Divestiture

A major Fortune 500 organization needed to divest a key business unit including all core systems and business processes. Our support included completing projects that ensured the secure separation of more than 20 specific business areas into two distinct go-forward organizations.

This effort included security architecture services to ensure that all core systems and applications were secure during and after the split, as well as the development of a new security program structure and the supporting policies, standards, and procedures.

**Key Challenges:** This was a large-scale, multi-year effort. Below were some key experiences that the team had to face.

**Splitting Up Isn't Easy** — Coming to an agreement on how to move forward as your organization is being split into different units requires frequent meetings and clear, concise explanations.

**Tight Timelines** — Scope may change, but the schedule often isn't flexible with these types of engagements. We had to manage getting everything done even though the transition date was set long in advance. This meant toggling between more resources or less scope, which is hard when you're talking about security.

**Large Team** — There were multiple consulting and services teams from different companies moving everything forward. Each team had different direct assignments but the same overarching goal. This can be difficult and requires clearly-defined accountabilities and responsibilities.

## Going Global

A growing biotech organization based in the United States needed to open operations in Europe. The initial program was immature and the additional requirements to do business in Europe led the organization to want to develop a more mature global security program.

Maturing the organization's security program included the complete development of a comprehensive security and privacy program from the ground up. This included the program charter, policies, and all key program functions including risk, incident, vulnerability management, and more.

**Key Challenges:** Building and maturing a security program from the bottom up included several challenges.

**Different Mindset on Privacy** — Europe requires that users have the ability to explicitly opt-in for every way an organization uses their personal data when it comes to privacy. In the US we often operate with the opposite mentality of one opt-in for everything, though this is quickly changing.

**Resource Availability** — This was a small organization with over-allocated resourcing in every aspect of the business. Getting in front of decision-makers was difficult, though we solved this with consistently scheduled and well-run communication updates and meetings.

**Antiquated Medical Devices** — Medical devices in healthcare and biotech organizations are often difficult to secure because of old or outdated operating systems. We needed to devise a sophisticated secure architecture in order to compensate for and address these issues.

## Our Customers Demand It

A funded and successful organization that sold business-to-business services with major brands needed a way to meet the security requirements of their customers. They were consistently receiving security questionnaires from these customers and did not know how to respond.

We helped with the tactical development of a risk management program that allowed us to centralize and organize all these requests, as well as what needed to be fixed in each situation. We then organized a strategic and tactical roadmap to improve the program over time, while simultaneously fixing time-sensitive issues according to customer requirements.

**Key Challenges:** Meeting specific customer demands presented unique challenges that needed to be addressed throughout our engagement.

**Took the Board Time** — The board in this organization needed to be educated on an appropriate budget to correct legacy security issues and build a best practice program. In the beginning, they were setting incorrect budgets.

**Resource Availability** — The organization did not have appropriate resources for any of the tasks in the business, let alone for security.

**Unlimited Cyber Liability** — Customers required the organization to have unlimited liability for security if a breach occurred, and they had difficulty getting cyber insurance that adequately protected them while improving the program. This was the primary driver that opened up a larger budget in the organization to enable us to move quicker.



## Rapid Growth

This organization was more than doubling in size over the course of a couple years. Their existing security program was continuously rendered outdated with each growth cycle and many of the same people that were involved in the security program when they had 10 people were there as they grew to over 200.

We helped with a series of engagements over time from initial program development to business continuity as they grew. The goal was always to keep the security program effort in line with the growth of the business.

**Key Challenges:** A rapidly growing organization presented unique challenges to program scalability.

**Not a Mom and Pop Anymore** — Many of the early people in the organization were still there later on as the organization grew. While their budgets and scope had grown, sometimes the organization still thought of itself as a small mom and pop organization.

**Resource Availability** — This is always a consistent problem in security, even more so in an organization that is growing so rapidly. To address this, this company ended up using our managed services in addition to professional services engagements.

**Lumpy Process Velocity** — They would receive 5 customer security assessments one month, 15 the next, and then 2 the month after. It was hard to properly resource the demands of the security program since their headcount was fixed while the demand was not. Moving to managed services helped alleviate this problem.

**Cultural Impacts** — As the company changed, so did its culture. Ensuring that the security effort did not impact this maturation in a negative way, took mindful planning through an effective awareness program.

## After the Security Breach

The wounds are still fresh from a data disclosure and ransomware attack. This public agency had recovered from the initial damage and some of the dust had settled. Now, they needed a multi-year plan moving forward to ensure that this never happened again.

We previously supported the organization with incident management services during the breach and their recovery from it. After the incident was remediated, we helped them with more professional services by creating a multi-year security program development plan and roadmap forward.

**Key Challenges:** We worked with the client to ensure the program and go-forward plan met all of their needs.

**The Wounds Were Still Fresh** — Many organizations after a breach are ready to move forward but are unsure of the concrete next steps. Organizations typically want to do everything immediately, and this is hard to do since there's a lot to finish. This is why a well thought out plan and timeline is so important.

**Progress Reporting** — The highest levels of the organization wanted constant updates on how the plan was being implemented. Rightfully so, but this takes a lot of time to organize and put together. We accomplished this by building a comprehensive communication and reporting system integrated into the security plan.

**Government Agency Considerations** — Everything is so visible in a public agency; it can be hard to get the true perspective of those involved. This is especially an issue in government agencies, but it can make having sensitive security conversations difficult.



## Security Accreditation (SOC2)

A large Fortune 500 organization was interested in becoming AICPA SOC2 accredited. The organization had only recently developed an information security program. Now they wanted to get it accredited because of direction from their board.

Our team developed the initial security program, as well as the process development and readiness testing. We did this to prepare them for the external organization that was going to perform their formal SOC2 audit.

**Key Challenges:** Preparing an organization for SOC2 accreditation provided several challenges for the team.

**Employee Turnover** — Turnover was high both inside and outside the security program, including resources that were required to perform in-scope processes for accreditation. We tracked this issue and ensured new resources were adequately and continuously trained on their responsibilities.

**Project Management** — We utilized a dedicated project manager from our team to lead these projects for this client, which was a newer concept for this organization. As a result, it took time for us to educate stakeholders on what our project managers were doing and why they were doing them.

**Quality** — When it comes to SOC testing or any type of accreditation, things can't just be done. Tasks need to be completed with accuracy and in a repeatable fashion. Ensuring quality and the appropriate attention to detail in employee work within an organization is a common challenge.



## Venture/Equity Investment

Another organization also faced dramatic growth, this time through capital infusion from outside investors. The organization's goal was to use this money to develop more mature processes throughout the business, including in security.

Our team was involved in the development of the entire security program, as well as the security architecture.

**Key Challenges:** Our team faced unique challenges in building a security program while keeping stakeholders and investors appropriately updated.

**Investor Understanding of Security** — Whether investors come through venture or equity investment, they often see security as insurance and something that can hinder growth. As a result, it can be difficult to get the appropriate budget needed to build the right program.

**Lots of New Team Members** — So many business functions were being spun up at once, it was hard in the beginning to get appropriate integration of security processes as the program was developed.

**Schedule** — When investors fund businesses, they often set the schedule for implementing everything early in the process before the scope of what the business needs is fully established. This becomes difficult to manage when the scope is larger.





## Board Had Invested in Security, Now What?

A large healthcare organization had experienced a small security incident a couple of years before and they invested millions in the security program as a result. Much of this money went into acquiring different security technologies. The security leader who did this was gone, and the board began to put pressure on monitoring the maturity of the program after this investment.

Our team conducted a best practice assessment of the security program and security architecture to understand current state, as well as develop a multi-year plan forward.

**Key Challenges:** Assessing and improving a security program that was dependent on technologies required a lot of time during the assessment period.

**Sorting Through Forgotten Toys** — While some state-of-the-art security technology was acquired, most of it was either not turned on or only minimally operating. This is almost always the case when a program depends solely on technology.

**Inefficient Security Architecture** — This was distressing for management, because they were spending a lot on security technology, but the architecture didn't reduce the company's susceptibility to many of the threats they faced. We were able to communicate this through the security architecture analysis we performed.

**Lack of Program Scope** — The security program charter was inappropriate, and many people inside and outside the program didn't know what their responsibilities were. This led to a lot of fighting amongst internal teams, leading to colorful and intense assessments.


**Lack of Policy and Process** — Many of the core program elements such as policy and process documentation were missing, so the definition of the security program was nearly non-existent. This may have made the assessment simpler, but our team had to educate employees and stakeholders about how and why effective security definition is crucial to an effective program.

**Lack of Risk Management** — Risk and vulnerability management were also significantly lacking. Because of this, the organization did not appropriately identify risk, which led to an inability to inform management about risk issues that could guide informed decision making. This meant that our multi-year roadmap ended up with a much larger budget than leadership expected, since they'd already spent a lot of money on all the wrong things.

## Conclusion

The security program development process varies according to every company's needs and contexts. Changes and proper development of a security program are often done in response to changes in an organization, whether because of exponential growth, an acquisition, or everything in between. The key to an effective security program comes in striking a balance between resources, compliance, and security.

CISOSHARE's security experts are ready to help organizations with all of their security development needs through ongoing and project-based contracts. With every company, we tailor our security program services to a client's requirements, business goals, and the regulatory requirements they must adhere to. Focus on establishing a security program that improves your ability to make informed security decisions and implement these decisions in an optimal timeframe.



Have an upcoming security project?  
Call us — we're ready to help.

[Schedule a Call](#)