

The Growth of First Factory: Scaling with Fractional CISO

Starting Small

Cybersecurity benefits from foresight and forward thinking. Like planting a tree, the best time to do so was yesterday. The next best time is today. The earlier you plant it, the sooner you may enjoy its shade.

First Factory has been forward-thinking on the role of a vCISO in its security program. They quickly identified the need for cybersecurity support as their clients diversified, their teams grew, and questionnaires from prospects began reaching their sales and technical teams. At the time, they were a smaller business and chose a one-person, part-time vCISO provider that suited them.

He helped them get started on their cybersecurity program and answer questionnaires, but retired before long. He recommended that First Factory contact Fractional CISO to continue their security journey.

Virtual CISO firms are able to provide more support to clients than sole proprietors can. Fractional CISO provides each client with a cybersecurity team consisting of a Virtual CISO Principal and a Cybersecurity Analyst.

First Factory's Cybersecurity Team

First Factory went from being served by one person to enjoying the benefits of a two-person cybersecurity team.



Dan Bjorklund, CISSP
vCISO Principal



Owen Wight
Cybersecurity Analyst

"We wanted to avoid the situation where an individual could leave us or be consumed with a bigger client. We also were comfortable with increased spend, not just for a Virtual CISO but the tools and breadth of experience as we kept growing," said First Factory COO Don Gregori.

Today, First Factory is served by Virtual CISO Principal Dan Bjorklund, CISSP, and Cybersecurity Analyst Owen Wight.

First Factory's cybersecurity team meets weekly and continuously drives cybersecurity program improvements, while identifying emerging risks and technologies that warrant new action steps.

Fractional CISO \ FIRST FACTORY

Executive Summary

First Factory went from being served by one person to enjoying the benefits of a two-person cybersecurity team.

Key Highlights:

1. Fractional CISO's customized approach has helped First Factory solve security challenges unique to its business.
2. Cybersecurity questionnaires are made easier and used to drive improvements to the program.
3. First Factory is already well-positioned to become SOC 2 compliant later this year.

"We like the fact that Dan has a military background; there is a process and a regimen that he has instinctively. He has really helped us see the course a lot more clearly in terms of where we need to go, how we need to get there, what we're working on right now, and how to deliver on it."

Cybersecurity that Supports the Business

While the previous vCISO had helped First Factory get their cybersecurity program up and running, the limitations of a one-person shop had begun to show. Notably, this CISO's prepared resources were designed as a one-size-fits-all, including much larger clients typically served. "With our previous CISO, there was a density to the policies, and they were harder to customize to our needs. Dan and the analysts have helped me, the non-technical one of the leadership committee, understand the pieces better than I did before, keep us focused on the high-yield tasks, and made it easier to add our brand's voice and tone to the work."

Fractional CISO is particularly focused on using cybersecurity to support First Factory's unique business plan and environment. "In most cases we're a natural extension of our clients' teams so whatever cybersecurity they want to have or insist that we follow, we do. Then there are also places where we are running projects for clients where we control the infrastructure and environments."

Implementing different sets of controls for different client teams is a challenge for any organization. Dan analyzed First Factory's and their clients' needs, threat environment, and selected controls to fit. Together, Don and his Fractional CISO security team built trust for clients by ensuring the environments and systems used to service them are secure.

Customized Solutions

One way that Fractional CISO customizes their services to suit First Factory's environment is through specific Incident Response (IR) exercises.

Instead of pulling IR scenarios off the shelf, Fractional CISO designs them to target real risks to an organization's business objectives. For example - one of First Factory's exercises explored a cyber attack that knocked out a critical piece of First Factory's infrastructure, without which they cannot serve their largest clients. Unique scenarios like this help organizations design practical, specific IR plans and can even help them identify the need for additional controls and protections in advance.

"[The Fractional CISO] team has helped give us the insight as to what is important, what is quick, what is large and painful, and how to remedy it. We've been able to accomplish that in a lot of areas and I think that's been terrific."

Questionnaires Play a Role

Questionnaires were a critical motivation of First Factory's cybersecurity story, and they haven't gone anywhere.

Fractional CISO helps First Factory with questionnaires in **three specific ways:**

1. Helping review and fill out questionnaires - identifying what controls the organization does and does not have, and what should be added.

2. Coach IT employees on how to complete questionnaires, enabling them to answer them faster and on their own in the future.

3. Give First Factory leadership the attention and time needed to address problems identified by questionnaires quickly.

"Business relies on these, we can't move forward with big projects unless these get done and get done appropriately. Anything recognized as a deficiency, we bake it into the cybersecurity plan and can trust [Fractional CISO] to guide us through it."

SOC 2 Sufficient

First Factory is now aiming to complete a SOC 2 Type 1 audit, and Fractional CISO has already begun work preparing the team for the initiative. Dan provided the First Factory team with a set of SOC 2 question stems to get them thinking about what's next.

Dan has taken initiative on the SOC 2 project by taking that set of questions and mapping them to the cybersecurity program First Factory has built with Fractional CISO so far.

"We've been able to take each question, understand if we have something in place for it, and know how to answer it. It has allowed us to feel that we do have these more mature policies and procedures in place and understand how they manifest when dealing with an auditor and what [evidence] we may need to create."



Don Gregori
COO, First Factory
(All Quotes)

First Factory's quickly-maturing cybersecurity program is already well positioned to be SOC 2 compliant by the end of 2023.

Picking The Right Virtual CISO For Your Firm Will Help Ensure Cyber Success

There are many different types of vCISOs to choose from. Organizations should pick one whose capabilities naturally align with their security and compliance needs.

Fractional CISO's roster of vCISOs and customized solutions ensures that every client winds up with a CISO and cybersecurity plan that supports their business plan.

For First Factory, that vCISO is Dan. The custom cybersecurity program has involved working out the tricky problem of implementing controls for client environments

that don't conflict with First Factory's environment, using questionnaires and incident response to drive security improvements, and positioning themselves for SOC 2 success.

"I do think that Dan and Fractional CISO have been extremely diligent and effective in walking us through things in a very predictable manner and I think it's been terrific for us."