NETWORK
ASSURED

How Much 10 Companies Paid their Virtual CISO in 2022

by Nathaniel Cole

VIRTUAL CISO COST BENCHMARKING FOR 2022: 10 CASE STUDIES

A virtual CISO (vCISO) service is not a one size fits all. It is a highly robust and versatile service that can be molded, customized, and tweaked to meet the end goals of an organization. This is not simply a service to assist an immature or early-stage security program, but a service that can help any organization at any point on the security maturity spectrum. At the end of this article, you will be armed with enough data to help make the best choice for your end goals and requirements.

The case studies selected for examination range across industries, sizes, and goals to provide a wide range of data points to compare. Within each case study, an overview of the engagement, scope, and additional notes will be provided to assist with understanding what may impact the cost of the engagement.

Virtual CISO #1: Global FinTech Maturation Assistance

For this engagement, the organization recently promoted a security leader to the role of CISO and was looking to rapidly mature its security program. Over recent years, the organization had focused on security compliance and attained two major certifications but was interested in shifting the focus from compliance to a secure posture. As part of this, strategic roadmaps were needed to be developed, based on completed gap assessments.

Furthermore, the organization wanted to shift reporting of security from strictly reporting to the technical teams to presenting and discussing security risk, exposure, and maturity with senior leadership and a subset of the board. As part of this engagement, a vCISO was hired to assist with developing the communication cadence, content, and style.

Industry: FinTech
Size of the Organization: ~500
Cost: ~$6,500 per month

Scope: Monthly retainer for services, guidance, and program development of 10 hours per month with monthly office hours over video for executive training. Service provides flexibility to focus on what the senior security leader would need assistance with which could include policy development, compliance, training, recruiting, or executive meetings.

Notes: Initial focus of the vCISO service was defining strategy and direction to build a sustainable security program that aligned with the organization's evolving business initiatives. Further goals were to promote a healthy security posture within the company through mentoring and coaching of the CISO and other key leadership. The initial contract was for one year with the potential to extend on a month-to-month basis at the end of the original contract.

Virtual CISO #2: Oil and Logistics Seeking Industry Expertise

The parent organization in the Oil and Logistics vertical wanted to improve the security posture of a smaller subsidiary that was operating in a highly regulated industry.

The parent organization's security team was not familiar with the vertical that the subsidiary operated in. The subsidiary was not fully integrated into the parent company's security program, which required local security resources. For this reason, a vCISO was brought in to help drive strategic planning, communication, and a culture of continuous improvement within the subsidiary organization.
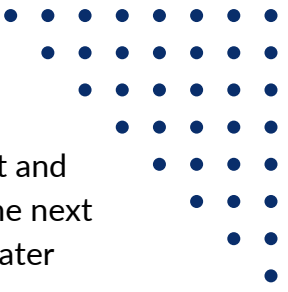
The vCISO reported to the parent organization's CISO but worked with the director of security at the subsidiary to better understand the operational requirements and needs of the subsidiary. The initial focus of the engagement was to review all policies and controls related to the information security management system, determine gaps, identify key improvements, and roadmap additional investments to assist with better meeting and exceeding security compliance.

Industry: Oil and Logistics
Size of the Organization: >3,000
Cost: ~$9,400 per month

Scope: Up to 20 hours per month with office hours over video chat to assist with program development, communication, and refinement of the information security management program. Services included policy development, compliance, training, reporting, marketing, recruiting, and sales support.

Notes: The initial focus for this engagement was to up-skill or train existing talent and further assist with defining the strategic direction of the security program over the next 18 to 24 months. The original contract was for a 6-month engagement that was later extended to be a total of 12 months. Further assistance was provided to evaluate vendors and solutions that could assist in streamlining security controls, evidence gathering, and governance of the security program. Some of these tools were adopted by the parent organization rather than just the subsidiary.

Virtual CISO #3: Interim CISO Service

A large healthcare technology company CISO provided notice and, while the notice provided was a 2-month notice, the organization was not able to hire a replacement CISO in the first 30 days. In a shift to provide more time to hire the right CISO for the company, the organization contracted with a large vendor to provide a vCISO on a full-time month-to-month contract. This allowed a one-month overlap between the outgoing CISO and the vCISO to provide continuity for the security program, team, and senior leadership.

Industry: Healthcare Technology
Size of the Organization: >2,000
Cost: ~$50,000 per month

Scope: Contracted for a vCISO to sit in the role of CISO for the organization while recruiting and hiring a replacement CISO. The scope included recruiting, training, staff management, evaluation of existing capabilities, and interviewing replacement candidates for the organization.

The primary goal for the vCISO service was to provide continuity, interview support, and a senior leader to continue to make critical security decisions as a full-time stand in for the exiting CISO. While additional guidance, assessments, and input on the current state of the security program were provided as part of the tenure, it was not expected or asked for by the company. The organization ended up contracting for 6 months with the vendor, with a 3-month ramp downtime period that consisted of a week to week trimming of total hours or time from the vCISO. During the 3-month ramp downtime, the cost eventually came down to $5800 and hours to 20 a month.

Virtual CISO #4: Rapid Maturation of a Security Program

A startup organization in the B2C technology vertical wanted to quickly ramp up its security program without investing in a full-time CISO within the organization. The organization engaged a part-time vCISO consultant to assist with writing, deploying, and communicating the initial set of policies required to meet ISO27001 certification. Further, the vCISO assisted with hiring 2 key security individual contributors to assist with the deployment of key controls and requirements for the standard.

As part of the back half of the engagement, the vCISO was tasked with providing the organization with a 12-month roadmap for continued maturity and plans for completing stages 1 and 2 of the ISO27001 assessment. Further, the vCISO assisted the organization's legal team in reviewing and addressing key requirements in the CCPA and GDPR data privacy regulations. The vCISO also assisted with writing key components of the privacy notice and legal disclaimers that were utilized on the company's websites to meet consumer protection requirements.

Industry: Technology Company
Size of the Organization: <200
Cost: ~$4,500 per month

Scope: Primary focus for this company was designing, building, and deploying an Information Security Management System to meet ISO27001 for the organization.

Notes: The contract was set for 10 hours per month, over the course of 12 months. The vCISO focused on developing a core set of policies and standards that could be deployed to assist with meeting the compliance standard. After about 3 months, the organization focused on interviewing and hiring 2 engineers to assist with the ongoing development, deployment, and maintenance of the security program.

The eventual goal for the organization was to hire a full-time security manager, but this was not accomplished before the end of the engagement, due to business restrictions. The organization was not able to meet ISO27001 before the end of the contract and was still working towards final certification shortly before the vCISO contract expired. The contract was not renewed, due to the belief that the engineers hired could inherit the program with the Director of Technology leading security until the organization was large enough to support a manager over the security team.

Virtual CISO #5: Digital Transformation Guidance

A mid-market bank in the US wanted to make the move from their colocation data center to a cloud-enabled posture. As part of this transition, the bank hired a bevy of consultants to assist with the transformation and one such consultant service was a vCISO.

The primary goal of the vCISO was to assist the existing Vice President of Information Security to review current policies, standards, and controls and identify required modifications to address the capabilities of a cloud deployment.

While many companies just lift and shift all existing controls and tools to the cloud, this bank wanted to make sure that the organization was maximizing its cloud investment with the right set of tools and controls. As part of this engagement, the vCISO assisted with the evaluation and selection of key security tools and controls to further assist a secure posture in the cloud. This allowed the organization to transition to a more agile cloud deployment while maintaining appropriate security controls to meet its regulatory and compliance requirements.

Industry: Banking
Size of the Organization: >1,000
Cost: ~$10,500 per month

Scope: Up to 20 hours per month in guidance, expertise, design, and deployment assistance of security policies, procedures, and controls for cloud deployment, as part of the transformation from an on-premises data center.

Virtual CISO #6: Mentor for Internal Promotion

A mid-sized technology company recently went through the exercise of replacing a retiring CISO. As part of this process, the CISO interviewed and selected a senior leader from the security team to backfill the role. While the individual hired for the CISO role had the relevant experience and technical skill sets, the organization and existing CISO wanted to provide additional assistance and mentoring to the new CISO. The organization engaged a vCISO service to provide the new CISO additional guidance, training, and assistance with building a communication cadence and plan.

Industry: Technology
Size of the Organization: >2,000
Cost: ~$12,000 per month

Scope: Development and training for an internal promotion to CISO to assist with executive communication strategy, strategic planning, evaluation of tools, assessment of the internal team, and development of internal business relationships across the organization.

Notes: The contract was for 6 months with the primary goal to ensure that the new CISO felt supported in the new role. This entailed making appropriate changes to the communication cadence and strategy that the previous CISO had developed, reviewing the current security program, and ongoing training. As part of this service, the vCISO provided additional mentoring and coaching related to engaging and connecting with peers across the organization. The service did not have a set number of hours that the new CISO could engage the vCISO for on a given week or month, but it averaged about 15 hours per month.

Virtual CISO #7: Operational Budget Refinement

A regional law firm engaged a vCISO consultant as part of a security and technology efficiency review project. The primary goal for this engagement was to review the operational budget for the security and technology team (separate engagement in the engineering and technology team) to identify how to better utilize the resources and budget. As part of this engagement, the vCISO conducted interviews, reviewed previous years' tool purchases, and gathered relevant data on the implementation efficacy of purchases and contracts. The vCISO utilized the data to provide recommendations for areas where budget efficiency could be improved. The efficiency gain could have been from tool overlap, tool underutilization, or areas of over-investment. At the end of the engagement, the CISO provided a report to the board on how the organization could better utilize the resources dedicated to the security program and an appropriate roadmap to smooth the transition.

Industry: Legal
Size of the Organization: <1,000
Cost: ~$15,400 per month

Scope: Provide expertise and evaluation of current operational budget across tools, vendors, services, and allocation of internal resources to provide actionable recommendations to efficiently utilize the security operational budget.

Notes: The contract was for a 6-month engagement that consisted of 20 hours a month, on average. While the primary focus was related to budget analysis the vCISO still provided guidance and input on operational improvements for the security program that included communication improvements, roadmap focus, and key threats that may impact the organization.

Virtual CISO #8: Regulatory Checkbox

A small financial investments company operation in New York engaged for a vCISO to meet key requirements, a CISO reporting to the board, of the NY DFS Part 500 regulation. As part of this requirement, a financial service company must have a CISO, either full-time internally or through a third party, who reports directly to the CEO and board.

While this company had a named CISO in the past, it did not see the need to keep a full-time CISO after a resignation was tenured and chose to engage with a trusted third party to provide the required reporting and title for the regulation.

Industry: Financial Investments
Size of the Organization: >500
Cost: ~$10,400 per month

Scope: Up to 20 hours per month to assist with program development, communication, and reporting to the board of directors. Services included policy development, compliance, interviewing, and performance tracking.

Notes: Initial plans included only reporting to the board and CEO on the status of the security program, but, as the vCISO became more familiar with the team and company, recommendations were provided on how better to posture security. Additionally, the vCISO became a trusted advisor and assisted with recruiting and hiring key personnel within the security team and technology teams.
The contract was for 12 months but was extended for another 12 months.

Virtual CISO #9: vCISO for a BISO

While the term business information security officer (BISO) is still new, this large retail organization saw value in providing security advisory services closer to a critical component of the business. Due to a new business division that was a deviation from normal operation, the CISO decided it best to implement a senior security role closer to the division to assist with implementing and managing security controls, policies, and processes.

In this role, the vCISO was responsible for representing the business division's interests, while guiding compliance or documenting deviation from corporate security requirements.

In this position, the vCISO worked with the business line leads to understand the goals, operations, and requirements of the vertical that the business line was operating in to better direct the security focus and ensure that security is implemented closer to the team.

Industry: Retail
Size of the Organization: >2000
Scope: Provide best practice guidance, security roadmap, sales support, evaluate and assist with implementation of tools and services to stand up a security program that could enable the business
Cost: ~$15,000 per month

Notes: In this role, the vCISO provided up to 40 hours a month of support for senior leaders in the business division. The initial contract was for 12 months to establish a working model that could be deployed on a full-time basis. During this contract, the vCISO assisted with hiring key security team members, implementation of tools, and some minor deviations from corporate security that required further documentation. To date, the organization has not replaced the vCISO with a full-time BISO.

Virtual CISO #10: Increasing Visibility and Awareness for Consumer Tech Firm

Like a few other case studies above, a smaller company needed to mature and increase its security posture but was not ready to hire a full-time CISO into the organization. In this case, a small company needed assistance with strategic planning, areas of investment, hiring, and program development.

Instead of hiring a very senior security leader full-time, this organization chose to hire a vCISO to lead the organization on this maturity. This allowed the organization to hire a security engineer and analyst to assist with the deployment and maintenance of key security controls, that otherwise they may not have had the budget for if they hired a full-time CISO.

Industry: Consumer Technology
Size of the Organization: >200
Cost: ~$12,000 per month

Scope: Assist with developing security strategy and awareness within the organization. Manage risk across internal operations, vendors, and software development. Rapidly improve the incident response capabilities of the business.

Notes: The contract was for 24 months, as the organization wanted to create some stability with their vCISO and did not see being ready to hire a full-time CISO in the short term. Initially, the vCISO came into the organization with no supporting technical resources and was tasked with reviewing the organization's posture, business goals, and legal requirements to build a strategic roadmap. This took about 6 months to complete, at which time the focus turned to hiring the two additional resources and implementing key tools and controls within the organization.

Summary

These case studies were purposely selected from across small and large organizations. No matter the size of an organization, there is a use case for a vCISO service to mature and improve the overall security posture of the business. No matter if the security program is just being stood up or is extremely mature, there is a use case for a vCISO to improve an organization's security capabilities.

It has been commonplace for CEO and other C-level executives to have mentors or advisors with years of industry experience to assist with strategic decision-making. While this has not been as prevalent in security, in recent years, there has been a significant increase in the desire of organizations to provide their senior security leaders with the support and advice needed to increase the overall security posture of the organization. This not only provides another set of eyes on the operational security controls and strategic investment, but it also provides the most senior security leader a sounding board to discuss, debate, and theorize on approaches and solutions to assist the organization.

For smaller companies, the vCISO service provides a way to bring in the senior security leadership that otherwise would be missing from the organization. This is a huge benefit in being able to leverage the experience and expertise of an executive-level security leader that can work with other senior leaders in the business to understand the current and future security requirements for the organization. This allows the organization to address those needs earlier and avoid large amounts of technical debt or re-engineering when the time comes to hire a full-time CISO.