NuHarbor SECURITY

The First 101 Days as a New CISO

A Chief Information Security Officer's Playbook

If you're a new Chief Information Security Officer (CISO) or taking on a new security leadership role, the first few months on the job are critical to your future success. You'll be judged, tested by your organization and staff, and put on stage to perform in front of your C-level peers. The precedent you set in your first 101 days will dictate how your organization perceives you and whether your tenure is marked by early challenges or confident navigation of the job you were hired to do.

This playbook for new CISOs outlines key initiatives and specific steps to help you find success in your first 101 days on the job.

Table of contents

Days 1–10

Take stock of the existing information security program

Start by taking inventory of all the components of your program, including direct and dotted line information security staff and responsibilities, established program capabilities and their maturity, and any available metrics on department performance. At a minimum, it's critical to take a cursory inventory of services in your first week. As you meet with other business unit leaders, you can start formulating a more vigorous and relevant information security strategy.

Get to know your colleagues

Don't skip this step toward kindling meaningful working relationships. If you're new to your company, be careful not to pass judgment during early discussions since you've had no experience with organizational politics yet. Use this time to build political capital by listening to your colleagues and showing empathy. Most importantly, take note of your colleagues' goals and objectives so you can support their success when you launch an updated information security roadmap and strategy.

Hold a department meeting

Taking action on this step is a must. Your team may be apprehensive about new leadership and how your strategy and management style will affect their jobs. Give everyone a chance to talk and ask questions. Be sure to listen, express empathy, and advise that you're still gathering information and not ready to make any decisions. This is a good opportunity to demonstrate your belief that everyone is on the same team and shares a common goal.

Review budget and metrics

Spend time dissecting your budget and breaking down capital and operating expenditures. You'll likely face questions over the coming weeks about the financial footprint of the information security team.

If a high volume of security and compliance spending has taken place before your arrival as CISO, you may be asked if capital expenditures can be reduced. If you're building an information security function from scratch, there may be less scrutiny given that an initial capital spend is expected, but it would be smart to appropriately set expectations if you anticipate heavy spending.

Let people know you exist

Information security is pervasive—it requires that you interface with all departments, not just IT. Putting people on alert and driving awareness of your role will serve as an invitation for people to reach out and discuss security topics and concerns, or simply start a dialogue. Early outreach helps to enforce that you're an approachable colleague.

"Most importantly, take note of your colleagues' goals and objectives so you can support their success when you launch an updated information security roadmap and strategy."

Days 11–20

Queue up an information security assessment

At the beginning of week three, schedule an independent information security assessment. Depending on company purchasing requirements, coordination of the assessment could take a few weeks in addition to an assessor's required lead time. This should be a holistic assessment of your information security program, not just a penetration test or vulnerability scan.

Find a quality information security advisor who can review your overall program posture using a well-recognized framework, such as ISO27001, and measure those controls in a business context so you can gain an accurate read on business risk and prioritize remediation plans accordingly.

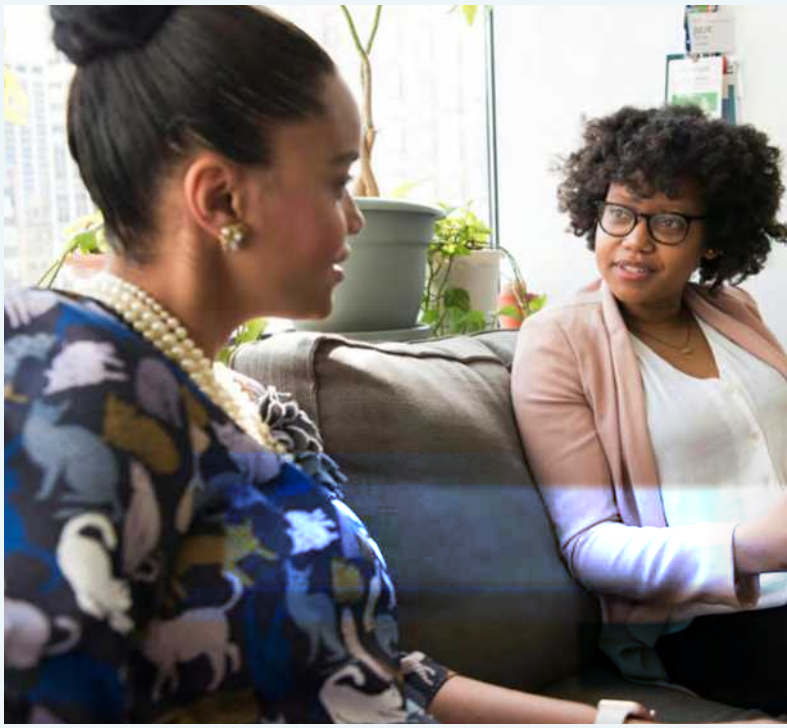
Hold one-on-one meetings with your team

Begin meeting with individual members of your team. Start with your direct reports before working through the org chart. If your team is so big you can't talk with everyone, make time to meet with frontline security staff even if it means skipping middle management tiers. Your frontline staff are the individuals who see issues and deal with problems and can offer a candid view of the challenges currently facing your new security domain.

During these meetings, you should aim to build political capital and trust within your team. Ask for informed, fact-based opinions on departmental risks and seek insight on how they could be mitigated. Use these meetings to establish your approachability by actively soliciting feedback.

Learn what projects or initiatives will be active within six months

In your busy third and fourth weeks, time permitting, start to understand new company initiatives or projects that will be active in the next six months. You'll be steering these upcoming projects and initiatives once you're fully embedded in your new position; building a strategy around their support will help you be purposeful and successful in your first 101 days. You'll gain context for your one-on-one meetings and get a glimpse into your team's plans and their tracking of associated risks.



Days 21-30

Prepare steering committee materials

If you have a security steering committee, you should begin preparing materials and framing the first meeting agenda. Your actual first meeting with the committee will come much later in your first 101 days, but if you're inheriting an existing committee, carefully structure the first meeting to get off on the right foot.

Note that there's increased complexity if the wrong stakeholders are involved (i.e., committee members don't have the appropriate seniority or experience). If you find yourself in this position, pause and critically evaluate whether you want to start over. Politically, it may be easiest to dissolve a legacy committee and develop sufficient political capital to rebuild. If you're starting a new steering committee for the first time, in addition to framing the first meeting format, you should also actively promote membership to desirable committee candidates.

Hold one-on-one meetings with business leaders

Start meeting with peers and business unit leaders. These relationships are critical to your ongoing success. In addition to gaining the trust of your company's business leaders, you should learn about their goals and objectives and incorporate them into your strategic plan and roadmap. This will help ensure your information security goals and initiatives directly correlate to business objectives. During these meetings, gather input on how the security team can help other business units.

Days 31-40

Review the operational security budget

Hopefully, you've obtained a solid understanding of your budget in the first two weeks. With a month under your belt, you're ready to start answering specific questions about your budget and the positive impacts of your spending. Your newly recruited financial analyst will validate budget planning and develop ROI metrics to demonstrate improvements in the finances of the evolving information security program.

Establish a program vision

Defining your program vision will shape your dialogue in the coming weeks. Based on your earlier conversations with business leaders, you should have an idea of what success looks like and how to help your company deliver on strategic goals and initiatives. While your vision may not be formalized, you'll have plenty of time to firm it up in the coming months. Consider this a prerequeset to developing an overall information security program strategy.

"Your actual first meeting with the committee will come much later in your first 101 days, but if you're inheriting an existing committee, carefully structure the first meeting to get off on the right foot."

Days 31-40

Begin your information security assessment

Kick off an independent review of your information security posture. While you may be qualified to perform the assessment, resist the temptation to do so. There's an opportunity cost in self-assessment: valuable program and relationship development. Additionally, the independent lens of an impartial party will lend creditability to the findings. During this assessment, it's critical to partner with your independent assessor and offer guidance to ensure the quality of the output.

The assessor is most likely new to your organization, so helping them adopt the appropriate business and security context will ensure an accurate measure of risk. An information security assessment without business context is just a gap assessment, and you need a risk assessment to prioritize remediation efforts. Depending on your corporate procurement processes, a 31-40 day start time may be unrealistic, but this assessment is a prerequisite to formalizing your information security program strategy and should be performed as soon as possible.

Inventory security team skill sets and establish development plans

As you talk with your team, holding one-on-one meetings and observing performance, take an inventory of both technical and soft skills. Soft skills are more challenging to define and measure, but tested frameworks (e.g., Lominger competencies) can help you evaluate. When creating a staff development plan, consider employee career aspirations to drive their skills development. You, as CISO, are an advisor and motivator, but development plans should be owned by the employee; they must be invested in the process and motivated to improve.

Employee underperformance or negative attitudes will create (or perpetuate) bad feelings on the team—you owe it to your top performers to fix this immediately. Don't spend all your time on the underperformers; each team member should receive equal attention. This may be one of your most important tasks, so take the time to get this right.

Days 41–50

Write, review, and maybe rewrite the information security charter

You'll want your charter approved by the CEO and board of directors, so it should be written at a high enough level that it communicates your mission and objectives, while providing enough detail to translate into an operational plan. Take the time to get this right the first time, because any changes or updates will need to be reapproved by the CEO and board. Many CISOs choose to have the charter approved by their security steering committee. If you're inheriting an existing information security charter, take the opportunity to review and make necessary changes or modifications.

Appoint team leaders

By now you've observed team performance and potentially identified a few stand-out leaders. Keeping in mind your information security program strategy and direction, it's time to put the right team in place to guarantee delivery. The leadership strength of those you select should inform the autonomy you afford them. Junior leaders will need more structure with work plans and project reviews. Senior leaders can work autonomously and will help you to coach those with less experience.

Be visible in established security projects

Whether you inherited a list of security projects or are preparing to kick off your own, judiciously select a limited number of important and strategic security projects to participate in. You may even choose to help a stalled project get back on track.

> **"You, as CISO, are an advisor and motivator, but development plans should be owned by the employee; they must be invested in the process and motivated to improve."**

While ramping up in your new role, you'll gain credibility and loyalty with your team as you demonstrate that you're there to help them succeed. Be careful not to overstep your project role and responsibilities; depending on your background and expertise, you don't want to be perceived as commandeering the project.

If you contribute too actively you may inadvertently skew responsibilities and derail progress. Establish personal participation guidelines for yourself. Your approach should be as a consensus builder rather than as a C-level overriding vote. There may be times when you need to pull your CISO card but only do it in dire circumstances.

Days 51–60

Review the budget for the second month

Review your budget again and you may see trends in your expenditures. You should now have enough information to start making informed decisions about your expenses. During development plan conversations, look for qualified team members to whom you can delegate budget monitoring responsibilities as a growth opportunity.

Meet with the steering committee or board of directors

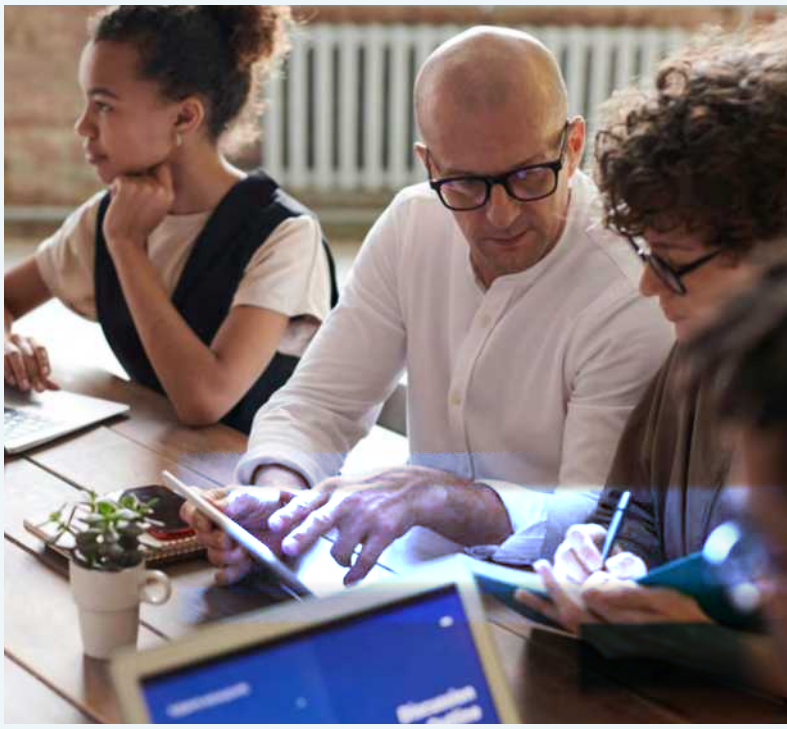
If you operate with a steering committee, you have flexibility as to when this meeting is scheduled because you drive the agenda and timing. Alternatively, if you have an opportunity to meet with the board of directors, you'll have to work around their schedules. Depending on when the board meets and how it aligns with your start date, it could make sense to skip presenting at the first board meeting of your tenure to ensure your first impression is strong, fact-based, valuable, and relevant to the overall business strategy.

Obtain approval for your security charter

It's time to get approval on the charter you drafted or updated in previous weeks. The date will be driven by the approving body (i.e., steering committee or board) schedule, but before requesting your opportunity, secure buy-in from any appropriate or influential reviewers. This will help establish support from the approving body to ensure a smooth approval process.

Form a security awareness team

This may be the most overlooked task in the new CISO's playbook. Continuous development of new and engaging security awareness ideas, content, and engagement is demanding. It's smart to enlist your marketing department to support creative content development and to structure effective messaging strategies. Take the time to give credit where it's due and keep that collaboration going. All members of the information security team are responsible for spreading your security awareness message. At a minimum, each should be required to deliver training annually.



Days 61–70

Formalize your information security program strategy

Two months for strategy development may seem lengthy, but you'll need time to craft your program vision and complete the independent information security assessment before stringing these data points together. Your strategy is ultimately a roadmap for delivering your program, and should include the following:

- A security maturity model for each cybersecurity competency you plan to develop in-house
- A cost-benefit analysis of internal investment versus partnering with a Managed Security Service Provider
- Capital and operational investment for cybersecurity competency development
- Operational investment for staff development and streamlining business operations

It's important to remember that information security is a risk management exercise, and risk mitigation costs time and money. In some cases, it makes sense to mature an information security competency to 90% of the potential capability because the last 10% is generally cost-prohibitive. Developing this roadmap and being purposeful about investment and ROI will generate traction for your future budget and improve your credibility with your executive peers.

Identify objectives for your information security team

Once your program strategy is complete, begin developing your annual information security playbook. This playbook should outline how your team delivers on your strategic objectives for the year, assigning team members in alignment with their respective professional development plans. Your playbook will also be your performance measurement and accountability data source.

Days 71–80

Monitor your information security program delivery

With your information security program strategy and playbook available, you can now drive and track the progress of your strategic deliverables, measuring your program's success. Most importantly, you have an early warning system that will let you know if your program begins to deviate from the plan. Consider these tools a component of your overall information security governance structure.

Days 81–90

Continue monitoring information security program delivery

Depending on the number of initiatives in your information security playbook and the volume of senior leaders, you may need to help junior leaders with their early efforts to gain traction.

Present at a company-wide meeting

If you have the opportunity, take advantage of the visibility and broad audience of an all-hands meeting to talk about the information security program, including what employees can expect and how to engage with the information security team. The sooner you can get on the agenda, the better, and by now you've had enough time to create supporting material about your program vision and security's role in advancing business objectives. While everyone on your team is responsible for spreading your security awareness message, this is your opportunity as CISO to introduce yourself and the information security brand to your company.

Days 91–100

Addressing business continuity planning and disaster recovery

If you have responsibility for business continuity planning (BCP) and disaster recovery (DR), it's time to perform or refresh your Business Impact Analysis (BIA) for BCP. The level of effort required will depend on the size of your business and executive support. If you need to convince other executives to reallocate resources to support BCP and BIA efforts, it may take longer to complete. While you gather support for your BCP and BIA plans, start collecting your asset inventory for the complementary DR efforts.

Day 101

Celebrate your first 100 days

You're on your way to building a top-notch security program. By this point you've completed significant tasks, including:

- Implementing an independent information security assessment of your organization
- Establishing solid working relationships with your colleagues, including other executives and the information security steering committee or board of directors
- Streamlining your information security budget
- Developing staffing development plans
- Creating an information security strategy and operationalizing an information security playbook

You've built a solid foundation for your company's information security function and positioned yourself well for future growth and recruiting and retaining top talent.

Make cybersecurity easier.

Learn more

AUTHOR

Justin Fimlaid

Founder and CEO
NuHarbor Security