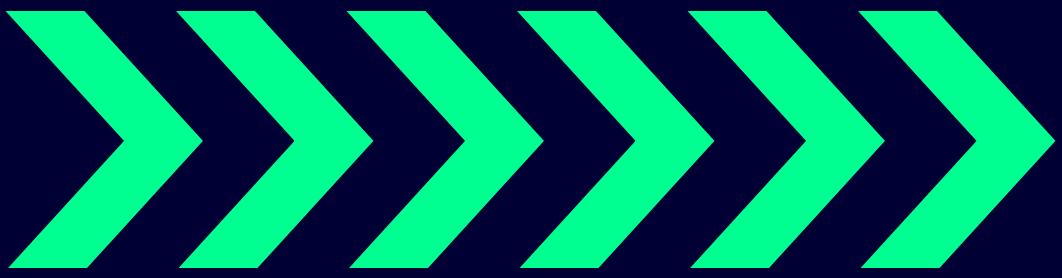
XM Cyber

Guide

The First 90 Days as CISO



Your Roadmap to Success

Introduction

They say you never get a second chance to make a first impression.

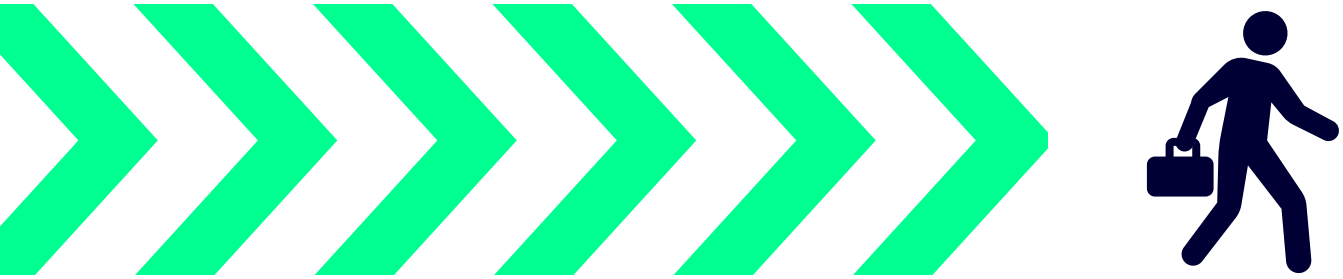
And accordingly, your first 90 days in a new role often serve as an indicator of your full experience.

But if you just came into a new CISO role, the stakes are elevated. With some estimates saying the typical CISO role lasts just 18 months, it's clear this role is full of challenges that are not for the faint of heart. With so much responsibility on your shoulders, and so much to account for, getting it right isn't easy. It takes a lot more than just dedication - it takes skills, both soft and hard, and a lot of planning to hone-in on the true security pulse and posture of the organization to optimize it.

That's why your first 90 days are the key to, and perhaps more appropriately, serve as the roadmap for, your success. "When leaders derail, their failures can almost always be traced to vicious cycles that developed in the first few months on the job," says Michael D. Watkins, author of the hugely popular book, The First 90 Days. So use this time period as an opportunity to lay the proper foundation.

The goal of this guide is to walk you through the steps you need to ensure your first 90 days are a success. By following these 15 steps, you'll set the groundwork for a fruitful experience.

To your success!



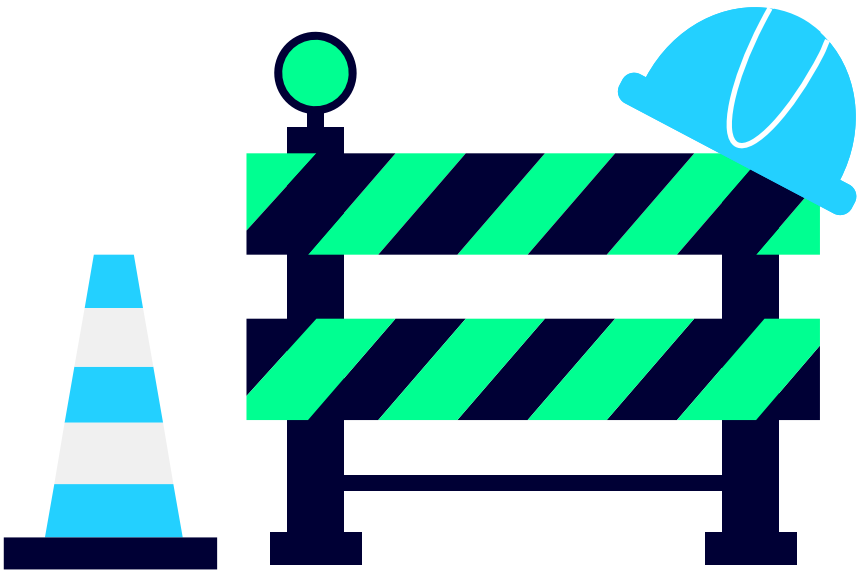
Month 1 - Laying The Foundation

01

Do Your Homework

So, you've just accepted an offer at your dream job, but it will be a few weeks before you begin. Now what? This time before you start is the best time to deeply research the company and review as much information as possible. Many companies share planning documents with new hires to help them acclimate as soon as possible. If you get such docs, make sure to cover the information therein to hit the ground running.

Also, start to decipher the organizational culture. Determine things like: how many hours do people really work? What are employee interactions like inside and outside the office? Are employees expected to always be available outside working hours? What is the organizational hierarchy like and what is the expected protocol for interacting with higher-ups? A great deal of friction comes from mismatched expectations, so head this one potential stressor off as soon as you can.



Determine the State of the Security Team

02

Get to know the state of the current security team and how to help them address any weak areas they may have. Look at your InfoSec, SOC, and GRC teams to start to assess their effectiveness, and alignment with business goals, and understand resource allocation of each. Understanding the nuances of each team can ensure you're making informed decisions from day one.

You also want to uncover why the CISO role was vacated or if it's a new role. If another CISO previously held the position, find out what went wrong and build a plan to address those issues.

03

Begin With the End in Mind

Picture yourself three years from now – what achievements do you want to have under your belt? What benchmarks would you like to have met? What programs would you like to see successfully running? Start to determine the vision you have for your program (which may be revised later on) and let these goals guide your future actions.

Step Back and Listen

04

There's a lot to do and you may want to jump in.

But instead, take a step back and listen deeply. Now is not the time for big (or any) changes. Instead, get to know your new organization and team. Practice active listening during conversations, focusing on both verbal and non-verbal cues to gauge underlying sentiments.

Take note of any recurring themes, concerns, or areas of ambiguity that may require further investigation or clarification. These cues will help you truly hone in on potentially problematic areas and build plans to address them. And hold all judgments for now – simply listen at this stage.

05

Ask What. Ask How. Ask Why.

Knowledge collection is an essential function of your job and there's a certain grace period in which you can be a "nudge", asking endless questions to extract information. After this time, people will simply assume (correctly or incorrectly) that you know – or should know – certain things. This period doesn't last long, so make sure to gather as much crucial information as you can.

Encourage open dialogue with thoughtful questions that prompt deeper discussions and insights. Seek clarification on current processes, policies, and practices to gain a comprehensive understanding of the security landscape. Challenge assumptions and probe for root causes to uncover potential vulnerabilities or inefficiencies.

What to Ask:

- ✓ What initiatives are already in process? What's been done to achieve them? How do they fit into the overall strategy?
- ✓ Are current processes and approaches more proactive or reactive?
- ✓ What are the greatest blindspots?
- ✓ What's the security culture like?
- ✓ How does the organization see the function of security? As a business-enabler or a hindrance to innovation and speed?
- ✓ What are interactions with other teams like? Is there a common language of risk or do teams work in silos, with their own benchmarks, SLAs, and KPIs?
- ✓ What compliance frameworks or regulations does the company meet and what's on the roadmap?
- ✓ When was the last time a vendor review was done?
- ✓ When was the last time a risk assessment was performed?

Month 2 - Getting Up And Running

06

Establish BC/DR Procedures

When assessing security, it's important to prioritize Business Continuity (BC) and Disaster Recovery (DR) plans. Evaluating how frequently these plans are tested and how aligned they are with current business priorities is essential for mitigating the risks associated with operational downtime or cyber incidents. Understand these procedures in depth to ensure your organization is prepared for potential disruptions.

Determine Organizational Risk Tolerance

07

Understanding the organization's risk tolerance is fundamental to your role, especially in the early days. Beyond assessing the state of the security team, it's essential to map business-critical assets and understand where the business is willing to accept, mitigate, or transfer risks.

Performing a full risk assessment early on will align security strategy with business priorities. Hands-on activities, such as shadowing field teams and observing day-to-day operations, can reveal gaps between documented policies and actual practices, giving you a clearer view of where real risks lie.

08

Assess Your Program and Components

Here's how to get started:

- **Review documentation:** Check out all relevant documentation related to the security program, including policies, procedures, guidelines, incident response plans, and risk assessments.
- **Inventory your assets:** Identify and document all critical assets, systems, applications, and data repositories within the organization. Include both physical and virtual assets.
- **Assess security controls:** Evaluate the effectiveness of existing security controls, like firewalls, intrusion detection systems, antivirus software, patch management procedures, access controls, and encryption methods.
- **Evaluate compliance:** Determine if your organization is compliant with relevant regulations, industry standards (such as ISO 27001, DORA, or NIST), and internal policies. Then identify any gaps to be addressed.
- **Conduct security assessments:** Perform internal or external security audits to identify vulnerabilities, exposures, weaknesses, and areas of improvement. (This step highlights the need for a strategic approach to addressing vulnerabilities and exposures in the most effective way possible. Check out our ebook, Operationalizing CTEM, for more on how to build that strategy.)
- **Evaluate security awareness training:** Review employee cybersecurity awareness training initiatives and assess their effectiveness.
- **Review Incident Response capabilities:** Evaluate your organization's IR plan, including processes for detecting, responding to, and recovering from incidents. (See the side bar for specifics on what to include in your IR plan.)

Your incident response should play a critical role in your first 90 days. A robust IR framework is essential to mitigate and contain the impact of security incidents. **Here's what it could include:**

IR Plan Evaluation:

Review and update the incident response plan to ensure it's up to date with current threats and includes clear escalation protocols, communication plans, and well-defined roles.

Tabletop Exercises:

Conduct tabletop exercises or simulations to test the effectiveness of the IR plan, identifying gaps in response, communication, and decision-making.

Post-Incident Reviews:

It's vital to assess how post-incident reviews are handled and how the lessons learned are implemented to improve future responses. A culture of continuous improvement should be embedded in the IR process.

Based on the assessment findings, identify and prioritize risks that pose the greatest threat to your organization's security posture. Develop a roadmap for addressing these risks and improving the overall security program.

09

Build Personal Capital and ID Your Champions

Identify individuals across departments who can help execute your goals and support and advocate for security initiatives. Schedule shadowing days to see the practical side of operations and uncover potential risks that may not surface in discussions alone. This practical understanding can significantly influence future security strategies. Build strong relationships with key stakeholders by demonstrating your expertise, reliability, and commitment. Leverage their influence to drive alignment, secure resources, and overcome potential roadblocks in your security strategies.

Start with:

CEO

It's important to understand what the CEO's impression of the security function has been until now: Do they see security as a business-enabler? If not, what can be done to change that perception? What are they missing in security posture reporting? What do they want to be communicated better and more comprehensively? Find out what they feel isn't working and begin to address those areas.

CFO

The CFO is your natural ally. They too see the world through the lens of risk and how to best reduce the likelihood of being impacted. They also need to ensure the bottom line is protected, and obviously, a massive part of that is adequate protection from cyber threats. Moreover, at the end of the day, they're the one you'll have to convince to get budget for your undertakings, so this is a critical relationship to get right.

CTO

The CTO enables innovation and ensures speed. Security has the reputation of being the opposite. Now is the time to banish that perception. This is the perfect opportunity to build a partnership and establish the right balance of security and innovation.

CIO

If you report to the CIO, you already know it's essential to get this relationship rolling on the right footing. Work closely with your CIO to understand, align with, and champion their goals.

VPs

It's important to know what's going on in each department, wherever feasible. Create a regular flow of communication with VPs from IT, HR, Marketing, R&D, Product Management, Operations, Sales, and more. Building strong relationships with department heads will help you gain insights into how security can support the business, not hinder it. Understanding these pain points and business needs early on will help you tailor security initiatives to drive value.

Define Your Metrics

10

Every security team and initiative should have measurable goals. Implementing Key Performance Indicators (KPIs) to measure effectiveness over time ensures that you can track improvements, demonstrate value, and justify the need for further investment in security initiatives. Metrics allow you to evaluate how effective your program is over time and provide crucial insights into what is working and what needs to be tweaked, implemented, or ditched. This is the key to making data-driven decisions and to monitor progress towards your goals.

Identify Key Performance Indicators (KPIs) to track progress, effectiveness, and impact in improving security posture. Define clear and measurable goals for your security program, aligning them with your organization's strategic objectives:
Here are some suggestions:

Less than 1%

of detected malware will be successfully executed

100%

of network intrusion attempts will be detected

Critical- and high-severity patches will be deployed no more

than 20% later

mandated by the information security policy

Less than 2

incidents will result from incorrect capacity planning and no incidents will be the result of failing to plan correctly

Determine the goals that are the best fit for your organization. Then establish a reporting framework to regularly track and communicate your metrics to stakeholders, highlighting successes and areas for improvement.

Month 3 - Putting It All Together

11

Earn Some Quick Wins

Rome wasn't built in a day and a well-executed security program doesn't appear overnight (no matter how badly some execs may want it to). But while it takes time for certain successes to yield tangible results, quick wins can be implemented to demonstrate your dedication to agility and bringing results.

Outlining a roadmap with short-, medium-, and long-term goals aligned with business objectives is key to ensuring progress is made and properly communicated. Start with small-scale projects or initiatives that can deliver tangible results within a short time frame. Focus early on efforts that address immediate security gaps, demonstrate your value, and build credibility.

Don’t be shy; as you meet executives, ask about the quick wins they’d like to see. Celebrate achievements with your team and stakeholders to generate momentum and support for larger, long-term security initiatives.

12

Work on the Cybersecurity Culture

Cultivating a security-conscious culture across the organization is one of your most important tasks. Security awareness training for employees, creating open communication channels, and encouraging shared responsibility for security can significantly reduce exposures caused by human error. You must champion cybersecurity not just as a compliance requirement, but as a core part of business success.

13

Plan Your Budget and Resources

Understanding the existing budget for security operations and making informed requests for additional resources is critical. This could include hiring more security personnel, outsourcing key functions, or acquiring new technologies. Tying budget requests to the risk assessment findings mentioned above will help secure the resources needed to enhance security posture. Presenting these in terms of risk scores and priority levels makes it easier for executives, especially the CFO, to understand the need and urgency.

Develop Long Term Strategies

14

Start tacking down your long-term security strategy.

Developing this multi-faceted game plan is a huge area for discussion and the finer details it includes are beyond the scope of this guide, but the main points it should cover are:

- ✓ Plans to address the changing cyber threat landscape and implications for your organization
- ✓ Assessment of your current cybersecurity maturity
- ✓ A framework for assessing and measuring cybersecurity maturity and growth
- ✓ Ways to improve reporting to the Board and C-suite
- ✓ How to improve security culture across the organization
- ✓ A plan for recruiting senior leaders into the cyber risk management governance process.
- ✓ Creating or assessing the risk governance process and implementing appropriate changes.

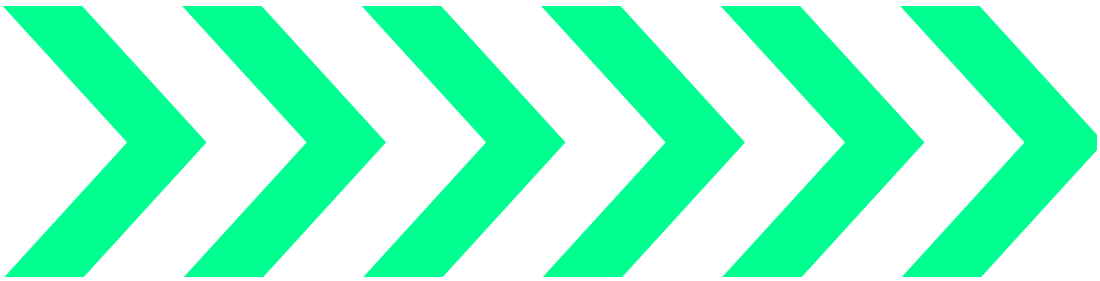
Include a timeline with measurable milestones and room for changes. This will keep everyone on track and enable continual assessment of progress.

15

Present Your Findings!

Present your findings of the last 90 days to your execs. Compile your observations, insights, and recommendations into a comprehensive report or presentation format. Here are some tips to improve your report:

- ✓ Use non-technical terms and keep it brief
- ✓ Present security as a business-enabler
- ✓ Talk about what's working and don't be afraid to say what's not working
- ✓ Use stats to back up findings
- ✓ Highlight key takeaways and action items
- ✓ Ask for feedback and input to ensure they have bought into the plan and everyone is aligned moving forward



Wrapping It All Up

Your first 90 days as CISO are exciting and challenging, filled with building bridges, assessing what you've got, and creating executable plans for enhancements. By staying focused on your goals of continuous improvement, you can establish an effective and impactful cybersecurity program for your organization.

Want to learn more about how to get set up for success in your new position?
Get a demo of the XM Cyber Continuous Exposure Management platform today!

XM Cyber

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort. Its XM Attack Graph Analysis™ capability discovers CVEs, misconfigurations, and identity issues across on-prem and all major cloud environments. It analyzes how attackers chain exposures together to reach critical assets, identifies key "choke points", and provides remediation guidance. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia, and Israel.