axio

100 Days to Build a Strong Cybersecurity Foundation

A LEADERSHIP GUIDE

Table of Contents

Introduction

The Chief Information Security Officer role, or CISO as it is commonly known, is an emerging executive-level leadership position that rightfully takes its place alongside other senior leaders in the organization. With responsibilities that traverse the organization and affect both internal and external stakeholders, the CISO position must establish a cybersecurity program that aligns with and supports the achievement of the imperatives and aspirations of the organization. This requires a vertical and horizontal approach: a vertical orientation whereby trust and cooperation with all levels of the organization are established and a horizontal orientation that spans across all organizational functions. Indeed, to be successful, the CISO must have an understanding and working knowledge of such varied capabilities as finance and accounting, legal, risk management, procurement, engineering, field operations, and of course, information technology.

Because effective cybersecurity requires contributions from everyone in the organization, the modern CISO can only be successful by leading at all levels of the organization.

But, in the short time that the CISO position has been established as a legitimate C-suite member, the challenges have grown more formidable. CISOs are under pressure from several directions at the same time. Most importantly, the threat landscape in which the organization operates is rapidly expanding, with attacks increasing in both velocity and impact. One such example is the rise of ransomware. Ransomware is a unique threat vector because, by design, it requires an adept response not only from cybersecurity and technical staff but also key decision-makers in the organization. Ransomware attackers have also broadened their motives. Recent attacks confirm more extreme profit ambitions, a desire to create political and social unrest, and an appetite for causing immeasurable damage to critical infrastructure that could have disastrous effects on the Nation's economy and the health and safety of its population.

At the same time, the internal challenges for CISOs are prevalent. Financial and budgetary constraints impede hiring staff, building infrastructure, and implementing cybersecurity projects. With fears of a looming recession compounded with geopolitical tensions, it's more important than ever to demonstrate value in both long-term strategic investments and tactical defensive operations. Cybersecurity continues to be viewed as a burden rather than a contributor to organizational value, requiring a near-constant tug-of-war to secure resources to execute the cybersecurity strategy. In fact, there is immense competition for internal projects, often requiring CISOs to make business cases for cybersecurity spending while competing with business expansion and revenue-generating projects that can more easily demonstrate contributions to the organization's bottom line.

Additionally, the regulatory environment is growing more declarative in nature, affecting the prioritization of projects and forcing a compliance mindset to permeate the cybersecurity strategy. The need for financial reporting of cybersecurity incidents has become top of mind for lawmakers and federal agencies And finally, CISOs are not shielded from customer demands. A more educated, cybersecurity-savvy customer base demands that suppliers and providers prove their commitment to cybersecurity as a condition of business. These demands conspire to force the CISO to walk a fine line between the organization's needs, the demands of customers and regulators, and the cybersecurity program. For seasoned CISOs this can be a career-defining challenge; for new CISOs it's imperative to establish solid footing with complete awareness of the potential barriers ahead.

About This Document

This document is designed to help CISOs and cybersecurity leaders establish the groundwork from which they can build, implement, and operate a successful cybersecurity program. It is useful for both new and experienced cybersecurity leaders, whether they are taking on new challenges, changing industries, or simply looking to refresh their approach as the organization evolves.

This guide provides the tools needed by all cybersecurity leaders to build a path to success. In the sections that follow, the leadership indoctrination process is broken into 30-day sprints; each intended to build (and maintain) critical relationships, skills, knowledge, and artifacts. Innovative approaches that expand beyond traditional cybersecurity program “to-do lists” are provided to jump-start accomplishments and ensure success. This includes exploring the essential role of risk management and quantification in building links between the technical ecosystem and the business language used by other senior leaders.

Using this document, new and existing CISOs can follow a structured approach that culminates in the

- establishment of critical relationships and collaborators.
- initiation of a cybersecurity strategy and roadmap (including prioritized near and long-term projects).
- creation of a quick-wins list that will include achievable goals to establish credibility and success.
- development of metrics to measure progress and communicate with senior management application of risk management and quantification tools and techniques.

The AXIO 30-60-90 Day Approach for CISOs

Things happen quickly in a CISOs world, and the planning horizon continues to shorten. There are many existing “100-day” guides available to CISOs that encourage a basic change management approach to achieve success on the job: build sponsorship, diagnose the current state, develop plans to address gaps and weaknesses, implement the plans, and measure effectiveness. And, while this is an established plan-do-check-act method for adopting an organizational change, it has potential limitations for CISOs.

Working with CISOs across many industries, the team at Axio has documented and codified an expanded approach aligned to the critical success factors that are vital to a CISO’s success within the organization. And, because cybersecurity is a continuous, ongoing, and challenging process, our approach does not stop there. Future success requires capitalizing on earlier wins, expanding influence, and building a coalition of the willing.

This guide is structured to provide defined and measurable artifacts that will help CISOs build a strong cybersecurity foundation in 100 days. Each 30-day sprint is focused on a specific endgame using Axio’s **"Three I’s" Approach**: In the first 30 days, you’ll *Immerse* yourself in the organization. In the second, you’ll *Initiate* the planning process. And in the final 30 days, you’ll begin meaningful *Implementation*.

In each phase described in this document, you will find three elements to help you on your journey: Objectives, Actions, and Artifacts. Objectives establish the things you should accomplish during the sprint. Actions itemize the to-do list of tasks that you need to plan and complete during the sprint. Artifacts define the tangible outcomes you should create or acquire during the sprint.

The first 30 days in Axio's 30-60-90 approach are critical to subsequent accomplishments throughout a CISOs tenure. This is the time where a CISO can plant the roots of cybersecurity leadership firmly in the organization to provide a foundation for achieving your program goals and meeting organizational expectations.

This sprint is considered the immersion phase of your journey. Depending on the size of the organization and the CISOs scope of responsibility, the work in this sprint may overlap into the next 30-day sprint. Because building competency in any role is a cumulative activity, taking longer in this phase is acceptable so long as you continue to make progress toward your 100-day goals.

First 30 Days: Objectives

Two core activities happen in this phase: understanding the organization and building the foundation of your program. The objectives of the plan's first 30 days are to:

First 30 Days: Recommended Actions

The bottom line for these 30 days is to better understand your playing field. This is the time to review your working knowledge of the organizational environment in which your program will operate. From these actions, you'll establish requirements on which you'll start to build your program. Let's begin by assessing your knowledge of the organization.

Establish your key stakeholders and begin relationship-building. Because the CISO role serves the entire organization—including customers and key business and external partners—it is vital that all entities with a vested interest in cybersecurity success be identified and established. This action will help you understand the different "consumers" of your role, their expectations, and what they can contribute to the success of the cybersecurity program.

The goal is to understand the role of each of your internal stakeholders in the organization, the scope of their responsibilities, and how they, directly and indirectly, intersect with the cybersecurity program. Document their expectations of the program as these may form requirements that you'll need to satisfy as the program matures. Ask your stakeholders about any major projects they have going on or are planning and how cybersecurity may affect them. And finally, gain an understanding of areas where collaboration and interaction will not only provide service to the stakeholder but improve the cybersecurity program. For example, working with Internal Audit may seem intimidating, but together you can identify areas of weakness that the program must address. Management's attention to audit findings can also help you get the funding and resources you need to be successful.

Internal stakeholders may include Legal, Risk Management, Finance and Accounting, Information Technology, Engineering and Operational Technology, Procurement/Purchasing, Sales, and Human Resources. Additionally, remember that senior management may have a separate (and possibly contradictory) set of expectations for your performance, so be sure to understand their requirements as well.

Equally important are external stakeholders. A survey of major supplier relationships, key customers, and other external parties (such as regulatory bodies) that are critical to the organization's success is in order. These relationships are easily identified during meetings with internal stakeholders, including your procurement or purchasing personnel. However, one important stakeholder that sits on the line between internal and external is the organization's Board of Directors. If you don't already, senior management can help you to understand the Board's level of involvement in the cybersecurity program to date and their expectations now that you are on board.

Determine the constraints, barriers, and boundaries of your program. Only in an ideal world do organizations operate without constraints, so you should expect you will have to operate within them as well. The cybersecurity program will be viewed differently by various stakeholders: for example, in a financial context for business leaders, a regulatory context by regulators and legal, and an operational context for engineers and field personnel.

As with all projects and programs, you'll be dealing with the same three constrained resources: time, money, and people. Take time to understand how the cybersecurity program has been funded in the past, the process for obtaining and approving funding, and the budget and financial resources you'll be inheriting. Be sure to familiarize yourself with the organization's project planning and funding process, including the financial tests (such as internal rate of return or net present value) to which your projects will be subjected. This will be important as you scope your program and prioritize projects.

It's also important to understand the human resources and positions assigned to your program. And remember, these may not be direct reports.

Cybersecurity is a horizontal activity, and many of the ground-level tasks performed by other departments are under your indirect guidance and influence. Your most vital resources may be in the IT department, in operations, and in support organizations like Internal Audit. Building a coalition of resources who will execute your strategy is one of the most critical factors in your long-term success.

Don’t forget the time dimension, either. Expectations for immediate and quick wins may be time-constrained, and the organization’s strategic direction may dictate what needs to be in place when. Your organization may also have near-term cybersecurity needs that have piled up. It’s imperative that you understand these needs and prioritize projects accordingly.

Understand your organization’s strategic plan and direction. Speaking of strategic direction, you must understand the organization’s strategic plan and its goals and objectives, both near and long term. Your cybersecurity program will need to align to these imperatives and will be time-bound by them. It may also dictate the prioritization of cybersecurity program elements such as new processes, projects, and tool acquisition.

Obtain and spend time understanding the organization’s latest published strategic plan. Begin to consider how this plan will influence your cybersecurity roadmap. Better yet, try to find ways that the emerging cybersecurity program can contribute to the organization’s achievement of one or more of these strategic goals. For example, if a new customer initiative is on the horizon, figure out how the program can enable improved customer confidence from a cybersecurity perspective. Customers highly value organizational investments in keeping their data and activities safe and secure. As you build your cybersecurity strategy and roadmap, ensure that it directly aligns to, references, and supports the organization’s strategic direction. This gives your cybersecurity strategy immediate credibility and will signal to management that you understand their direction and are a willing contributor to enabling their vision.

Study the organizational structure. Whether you’re new to the role or not, you presumably already know a lot about the organization if you hold the key role of CISO. But, a deeper dive into the organization’s structure will equip you to build a cybersecurity program (or programs) that encompasses the different—and sometimes diffuse—environments that exist under a single corporate canopy.

Different business units or lines of business (LOB) could have vastly different and sometimes conflicting cybersecurity risk profiles and requirements relative to their unique operating constraints, market environment, regulatory requirements, and strategic objectives. Each LOB may also have its own Board of Directors. This is often the case with larger manufacturing and energy companies. For example, an integrated energy company may comprise inherently risk tolerant LOB's to produce energy (think natural gas or oil drilling) and risk adverse LOB's to transport energy (think natural gas or oil gathering, transmission, and delivery). These variables may require you to plan and operate different cybersecurity programs for each LOB.

Additionally, you may encounter vertical differentiation. For example, the general computing environment that supports enterprise and business applications may be separated (both physically and logically) from field operations where smart technologies are used to operate assembly lines, manage pipelines, or deliver vital services such as water. The cybersecurity program for the Internet-facing IT environment may vary significantly from the closed-network, field-technology-driven operational environment that includes significant levels of firmware-driven devices. In reality, you may be required to build and operate programs for both environments simultaneously.

As you start to form an idea of the program structure, now is a good time to understand the risk profiles of each of the LOBs and the different operating environments. This may help you decide how to prioritize one over the other as you implement your program.

Gain an appreciation for how your organization manages risk. Speaking of risk, it's essential to view cybersecurity as a core risk management activity that today forms a substantial component of the organization's enterprise risk management (ERM) process and program. Several elements of risk management are important to understand at this stage. First, start with reviewing and understanding the ERM process and how you will be expected to integrate cybersecurity risk. Determine what requirements you may have to assess regularly, measure, and report cybersecurity risk into the ERM process and in what format.

Next, gain an understanding of the organization's risk "measuring stick." By this, we mean that you should understand the qualitative and quantitative tools the organization uses to measure risk. All organizations define a set of formal or informal risk tolerances or parameters to guide decisions about which risks are acceptable and which need attention. As with all risk-related activities, the cybersecurity program must also conform to this organizational risk appetite. And note again that risk appetite could vary widely within large organizations that operate in different vertical spaces. For example, integrated energy companies might be more risk-tolerant in energy exploration vs. energy delivery. With that in mind, you might have to alter how you measure cybersecurity risk depending on which line of business the risk emerges.

And finally, part of determining what constitutes acceptable risk is to look at the risk in terms of impact: how does it ultimately affect the organization? Your organization may have a specific risk quantification process that they use to translate a qualitative expression of risk (such as "low" or "moderate") into business language that can be used for decision making (such as "this risk could result in one million dollars in damage if realized"). This is especially important because estimating likelihood for cybersecurity risk events may be difficult. And, you may be required to use a reliable risk quantification method if your organization either has or will be acquiring cyber insurance.

Obtain an understanding of the IT environment and technical debt. While cybersecurity applies to people, processes, and technology in the organization, the technical infrastructure is by far the most integrated with the cybersecurity program. It is at once both the target environment of your cybersecurity program and the environment in which you will deploy a large portion of your cybersecurity tools and controls. Understanding this environment will be vitally important in developing a relevant and effective cybersecurity program.

Now is the time to survey the IT environment and form a functional picture of its layers, technologies, personnel, and projects. Develop a working knowledge of the specific technologies being used and their inherent vulnerabilities. For example, if you find yourself in a legacy environment, it may be easier to draw boundaries, but it may be subject to more inherent and age-related vulnerabilities. On the other hand, if the organization has embraced cloud technologies and anything-as-a-service, the security controls may have become more advanced, but your ability to get your arms around where the environment starts and ends may be more difficult. Be sure to understand all ongoing and planned IT projects (and, if possible, get a copy of IT's project roadmap). Because of the overlap between cybersecurity and IT, you'll want to determine which projects can help you, which ones you'll need to influence, and ones that you might become a barrier to.

When you're surveying the IT environment, don't forget to assess IT processes that you'll share with your IT colleagues. For example, traditional IT processes such as change management, configuration management, and asset management are essential intersection points between cybersecurity and IT operations that require a collaborative strategy and approach. And, your cybersecurity roadmap will likely include projects, processes, and technologies that overlap the IT environment, so you'll need to get IT leadership onboard.

Finally, try to estimate the organization's technical debt. As previously noted, legacy infrastructure and software may amplify your cybersecurity risk, especially if the organization hasn't been effective in updating to current versions of software and firmware or is operating legacy infrastructure. If the technical debt is large, it may also be an indicator that the organization traditionally under-invests in technology—a dangerous sign for your cybersecurity program if indeed, your roadmap includes significant technology acquisition needs. At the very least, knowing this may help you get a jump-start on developing bullet-proof justifications for the technologies you need to make your program work.

Now that you understand the organization—with all of its good and bad—let's use that information to shape and form the foundations of your cybersecurity program. But you'll need additional information to get that done. The following actions will help you gather what you need.

Get familiar with the organization's key cybersecurity capabilities. Your organization likely has at least a basic cybersecurity program in place. As you design this new program, you'll need to know what core capabilities exist and the degree to which you can build on them. Existing cybersecurity staff can certainly help with this exercise but remember that IT generally may have existing responsibility for these capabilities, so you'll need to expand your reach to gather useful data.

Baseline capabilities you'll want to inquire on include Asset Management, Identity and Access Management, Vulnerability Management, Change and Configuration Management, Supply Chain Risk Management, Network Security and Monitoring, Data Security, Situational Awareness, Incident Management, and Business Continuity/Disaster Recovery.

If you're lucky enough to find sufficient evidence that these capabilities are in place, you may want to ask some additional questions to determine how "real" these capabilities are—are they being used, managed, measured, and updated? Some questions you can ask to determine this include:

- Are the processes associated with these capabilities documented?
- Are specific roles assigned responsibility for the processes?
- Are the processes supported by policy?
- Is there a plan in place to guide the capability and associated processes?
- Is the effectiveness of the capability measured regularly and adjusted?
- Are the capabilities pervasively known and understood across the organization?

Review the organization's cybersecurity governance approach. You might not have time in this phase to dive deeply into the organization's internal control structure, but you can do a cursory review of how the organization approaches cybersecurity governance and identify what artifacts they have produced and implemented. Of particular importance, obtain all policy and procedure documents that relate to cybersecurity and IT governance. Review them for content, level of approval (senior management, Board, etc.), and last updated date. This will give you a sense of whether the organization is serious about cybersecurity and if you can use this foundation to jump-start your program.

Create a cybersecurity tool inventory. Many cybersecurity capabilities are tool-enabled. Building on the capability inventory you created, you'll want to know what investment has been made in cybersecurity and related IT tools that may be relied upon to implement your program. Additionally, this inventory might identify gaps in tool coverage, tools that are at their end-of-life, and duplication in toolsets that may need to be rationalized. In fact, helping the organization sort out the tool inventory could be a quick win for your program. This is often the case with monitoring capabilities. For example, monitoring tools are typically procured by both IT and cybersecurity personnel (often for the same purpose) and can be difficult to configure, which makes them prone to underuse in favor of the next-best thing.

At a minimum, you should find solutions in place for a privileged access management, vulnerability identification, IT service management, network and infrastructure monitoring, identity and access management, data loss preventions, etc. Your organization's toolset will vary widely, but at this point, it is sufficient to understand what you already have, whether it is operational (i.e., being used), whether it will fit into your emerging strategy, and what gaps you might have to plan for in your roadmap.

Understand your existing security architecture and related technologies. As you did with the tool inventory, it's imperative at this stage to make sure you understand the existing defense-in-depth security architecture and associated technologies. Create a working inventory and diagram and begin to identify potential gaps. The list of technologies and capabilities you should find in place is vast but includes:

- Intrusion Detection/Intrusion Protection
- Identity and Access Management (IAM)
- Privileged Access Management (PAM)
- Firewalls
- Virtual private network gateways
- Web gateways and reverse proxies
- Security-focused network segmentation
- Email spam and security filtering
- Endpoint Detection and Response (EDR) capabilities
- Security operations management technologies and capabilities
- Log aggregation technologies
- SIEM solution or near-SIEM
- Training and awareness learning management platforms (LMS)
- Wi-fi and mobile computing security

Also, it's important in this phase to begin documenting any outsourcing arrangements or *security-as-a-service* that may be in place. Pay special attention to any terms and conditions that you may have to operate within as well as the length of the agreement and the cost. You may want to also identify any early termination clauses in case you decide the current services are not a good fit for your cybersecurity strategy. (Be sure to budget for any early-termination costs if appropriate.)

Establish your initial program goals, objectives, and strategy. You've collected a lot of data and built many relationships in the first 30 days of the program. If you haven't done so yet, it's time to start developing a strawman set of cybersecurity program goals and objectives and sketch out a strategy. There are many guides available on the Internet that can help you structure your planning so that you create clear goals, align them with program objectives you want to achieve (and when), and support detailed plans and tasks.

Don't worry too much at this point about working within a structured planning framework. In the next 30-day phase, you'll select one or more cybersecurity frameworks that will guide the program through implementation and maturation. At this point, you can just simply start to use the capabilities you've already defined to build your strategic planning structure. For example, you'll need to build a strategy for *threat and vulnerability management*. In this broad category, you can associate all of the data you collected in this sprint: policies and procedures, roles and responsibilities, supporting tools and technologies, supporting security services, threat feeds/sources, etc. You can also start to articulate gaps. What tools are missing? Do we need additional sources of threat information? Do we need additional tools?

Also, be sure at this point to consider how the organization's structure will affect the strategy (if you'll have different LOB's and/or more than one cybersecurity program) and make direct connections where you can between your emerging strategy and the strategic goals of the organization or specific LOB.

What is important at this stage is to take everything you've learned in these 30-days and start to analyze and organize it as you move into the *initiation* phase.

First 30 Day Artifacts

- Documented expectations for each key stakeholder
- List of stakeholder projects (and in particular, IT projects)
- Current cybersecurity budget and staffing model
- Organizational project planning and justification process
- Enterprise risk management process/artifacts
- Organizational risk tolerance/risk quantification process
- List of ongoing and planned IT projects (IT roadmap)
- Core cybersecurity capabilities list and initial gap assessment
- Cybersecurity and IT governance documents (policies, procedures, standards)
- Cybersecurity tool inventory
- Working inventory and diagram of security architecture and related technologies
- Documented initial program goals, objectives, and strategy

In the first 30 days, you spent time understanding the organization, forming important relationships, taking inventory of your resources, gaining awareness of potential barriers and constraints, and documenting the current capabilities and technologies on which you can build. It's now time to take that information and knowledge to form your path forward.

This sprint is the initiation phase of your journey.

In the second 30 days, you'll commence the hard work of laying out your program goals and objectives, consistent with a guiding framework and supportive of an emerging roadmap of priorities. You'll also take a deeper dive into the current state of the organization's cybersecurity capabilities to understand where the most critical gaps exist.

At the end of this sprint, you'll be able to provide management with a detailed reporting of where you are, where you intend to go, how you'll get there, and how you'll measure your progress. And don't forget: in this sprint, you must confront how much this investment in cybersecurity improvement might cost.

Second 30 Days: Objectives

The objectives of the second 30 days center around designing, framing, and documenting activities. They include:

Second 30 Days: Recommended Actions

The honeymoon is over. It's time to focus on demonstrating value to the organization through the practice of cybersecurity. So, let's build a program and provide a vision of future success.

Select a guiding framework. This action sounds relatively simple but can be deceivingly difficult. The framework you decide to use may not entirely be your choice. Regulatory and compliance demands (for example, FFIEC-CAT for banking and finance), the industry sector you operate in (ES-C2M2 for the electricity subsector), existing or desired certifications (such as ISO 27000 or HITRUST), strategic initiatives (future government work requires CMMC or FedRAMP competence), and your organization's preference may be a few of the constraints that you need to consider. And, remember that you may need to embrace a multi-model environment whereby you use more than one framework concurrently.

At a program level, many organizations have embraced the NIST Cyber Security Framework (NIST CSF) as a generic structure to frame the scope and boundaries of a cybersecurity program. As it was designed to be industry-agnostic, NIST CSF can easily be adapted to integrate with your organization's specific directives and can be implemented at a functional level through many different control sets.

As we're discussing control sets, you'll also need to think about which framework of controls you'll need to manage at a practical level. If your program framework is more aligned to regulatory, compliance, or certification objectives, your choice of control set may be limited to those that support the objectives. For example, if your organization is attaining ISO 27000 certification, you'll need to ensure that all prescribed practices and controls are covered. In reality, general control frameworks such as the NIST 800-53 Security and Privacy Controls for Information Systems and Organizations are universally reflected in many compliance and certification frameworks, so you might not need to do much translation.

Remember, whatever you choose is going to permeate all of the remaining actions in the second 30 days because you'll be building your program aligned with these framework constraints.

For this reason, it is imperative that you spend sufficient time and energy in this task to understand your organization's requirements, inventory and evaluate the existing body of frameworks and controls, and select those that most sufficiently cover your emerging program. It's also a good idea at this phase to confirm your selection by discussing your approach with representatives of your Compliance Office, Legal, Risk Management, Internal Audit, Insurance, and others—especially those who routinely deal with compliance requests. Getting their input now may save you from having to rework your strategy and program later, which will likely come at the expense of moving your program forward.

Assess your capabilities at a practice level. In the first 30 days, you gained an understanding of the organization's cybersecurity capabilities and potential gaps. In this sprint, your objective is to perform a deeper practice and control level examination to understand the degree to which the organization is performing key cybersecurity functions. Just as you chose a framework to help guide your strategy and program development, a critical first step in assessing your capabilities is to choose the right assessment methodology or tool to develop your baseline. Remember: just as you may have decided to select more than one framework, you may find you need more than one assessment methodology or tool. In the end, your goal here is to determine how well the organization is already performing relative to your guiding frameworks.

Before you start off into the world of available assessment methodologies and tools, be conscious of the potential investment (in both money and time) that you may need to make. If possible, make use of the results of any recent assessments that may have been performed to form your baseline. This exercise is meant to give you a better, more independent understanding of the organization's current state so that you can quickly use it as input to your planning process.

Keep in mind for the long-term that there are some excellent multi-model assessment tools that collect generic information about your environment, practices, and controls and present the results in the context of more than one framework. For example, tools like Axio360 will help you collect information and then view your results at a programmatic level (i.e., in a NIST CSF context) and at a practice/control level (i.e., in a C2M2 context). These types of tools are most beneficial in not only providing a capability baseline but also in providing further input to strategy and roadmap priorities. In addition, if you have very specific regulatory or compliance obligations, most sponsoring organizations provide their own methodologies for assessment. These can be a useful addition to your assessment toolkit that will give you a head-start in future compliance reviews to which your organization may be subjected.

If you decide to select a tool partner for the long run at this stage, you can still perform a sufficiently brief assessment that will give you the information you need for planning purposes. For example, you can perform a self-assessment in a group setting with relevant stakeholders in as little as a half-day commitment. Or, if you want to ensure full cooperation and independence, many assessment methodology and tool vendors can perform a guided quick-start assessment activity that will provide you with an excellent foundation on which to build your initial strategy and future improvement activities.

Build your initial strategy and plan. At this point, you have collected a significant amount of information that provides vital input to your strategic planning and road mapping process. Strategic planning is a structured and involved process that allows you to clearly articulate what you intend to accomplish and how. It is a continuous activity that you are baselining at this point.

- *Start with developing a brief mission statement.* The mission statement should clearly articulate the purpose of your cybersecurity program and provide an overall achievement target for your program's goals, objectives, strategy, and roadmap. In other words, if you achieve your goals and objectives, your mission statement will be accomplished.
- *Itemize your strategic planning categories.* These are the specific areas in which you will develop strategic goals and related objectives. They may align to framework domains or categories or be developed in the specific context of your organization. They can be programmatic areas (such as risk management) and technical (such as vulnerability management). A few areas to consider are:
    - Threat awareness and acquisition
    - Training and awareness
    - Endpoint detection and response
    - Defense in depth architecture
    - Situational awareness and monitoring
    - Security operations/Security operations, automation, and response (SOAR)
    - Third-party risk management
    - Identity and access management
    - Vulnerability management
    - Data security and data loss prevention
    - Operational technology
    - Insider threat
    - Risk management
    - Program management
    - Regulatory and compliance management

- *Develop initial strategic goals.* Strategic goals are the "what" your program intends to accomplish. Implicitly, your goals should reflect any gaps you identified during your information gathering, as well as to ensure areas of strength continue to be supported and improved. For example, a strategic goal in the area of vulnerability management could be to "improve the timely identification of vulnerabilities." Or, a simple goal for insider threat might be to "develop an insider threat program."
- *Outline initial strategic objectives.* Objectives define "how" you are going to achieve your strategic goals. This exercise should identify two or three objectives for each strategic goal that you set. Objectives should start with action words and be measurable. For example, a strategic goal of "Create a culture of cybersecurity" might have objectives such as "Implement a phishing training program" and "Develop a monthly cybersecurity communication newsletter." Make a note of any tools, technologies, support services, and people you may need to achieve these objectives—you may need to include them in your roadmap. Remember: your strategic objectives reflect that you understand how to actualize your strategy, so make them clear, understandable, and achievable

Clearly, you'll need to iterate on your strategy, so establish a best first-effort in this task. You'll produce a tangible artifact that you can begin to socialize with relevant stakeholders and improve upon. And, now is also a great time to ensure your strategy aligns with and supports the organization's strategic plan and mission. Misalignment could be a signal that your program will not add value, which could create a formidable barrier to success.

Create a strawman roadmap. The roadmap is your strategy in action and priority. It articulates in a sequential and time-specific way the actions you need to take to actualize your objectives and achieve your strategic goals.

In this exercise, you'll take the output from your strategic planning effort and lay out a vision for the near-term and long-term of the major projects and activities you'll implement. You can organize the roadmap in the same categories as your strategic plan, or you can simplify and use generic categories such as governance, metrics, people, processes, tools/technologies, and external services. Choose a timescale that is used by the organization, typically monthly or quarterly, for periods of 1 to 3 years. For each item in the roadmap, document a proposed start date and a commensurate end date, taking into consideration the length of time the activity may take. Keep in mind, if your program must account for different LOB's or a separate operational technology implementation, you might consider creating roadmaps specific to these different efforts.

If you have access to the organization's strategic plan and/or project plan, you can also consider overlaying this information to your roadmap to identify potential points of synergy or conflict.

Consider the organization's timing of key projects and efforts that might impact your roadmap. Make sure you identify the tools and other supporting things you'll need. For example, if you are looking to implement a vulnerability management program, your roadmap must account for all relevant actions, including tool acquisition, proof-of-concept, implementation, and operation alongside developing processes and practices.

Build a budget. So far, you've been relatively able to plan without fully considering cost constraints. At this point, a realistic financial view of your strategy needs to take shape to inform how you execute your vision after the first 100 days.

A calculation of your funding needs at this stage is a good way to gauge the organization's willingness to invest in strong cybersecurity measures to avoid disruptions to its operations and future vision. It's unlikely your financial wish list will be embraced without significant iteration and consideration, but at this point, you'll want to at least have an idea of the realm of possibilities. By design, this exercise will help you understand the organization's financial limitations so that you can adjust your strategy and roadmap accordingly.

As you begin to quantify your vision, don't forget to examine the existing cybersecurity operational budget. There may be items that you've inherited (such as long-term contracts for services or maintenance on tools) that are not avoidable and will have to be considered in your vision. Additionally, you may have shared expense responsibilities with your information technology colleagues (particularly for monitoring tools that routinely traverse many departments or capabilities such as multi-factor authentication that may be packaged into other technology infrastructure) that need to be coordinated.

As you are creating this initial budget, it's imperative to separate capital and expense items as well. Many cybersecurity investments can be capitalized with benefits to the organization, so be sure to identify these items separately.

Lastly, this budget exercise can have a tremendous impact on your early credibility in the job, so give it considerable attention. In fact, itemizing a "quick wins" list of low-investment, high-payoff objectives from your strategy can strike the right tone as you prepare for the challenge ahead. And, as you begin to socialize your initial financial requirements, remember to remain flexible and willing to revisit your roadmap and make adjustments in priority and timing.

Develop an initial set of metrics. How will you know if your approach, strategy, plan, and program will be successful? How will other stakeholders in the organization measure your success and the success of your program?

The interesting challenge for cybersecurity professionals is to assert success in the absence of clear evidence. That is, success in cybersecurity is often a measure of what hasn't happened instead of what has. Often, this means measuring effectiveness by looking back after an event. Your program is going to need solid success measurements to thrive, so developing sound metrics now that support evidence of progress is important.

There are a few ways to approach this task. Your senior management and Board may have information needs that masquerade as “metrics” that you’ll need to report on. Embrace these requirements by documenting them and deciding how you will measure them in a reliable and consistent way. Often, these requirements amount to simple “counts” of things such as “the number of vulnerabilities that were patched in a specific period of time” or “the average time it takes to patch a critical vulnerability once identified."

At any rate, start with simple but informative metrics. Follow a structured approach to develop these metrics as follows.

- *Develop measurement objectives.* Start by documenting what you and your stakeholders want to know. These needs can be expressed in the form of a question, such as “How quickly are we remediating known critical vulnerabilities?”
- *Develop corresponding metrics.* For each measurement objective, create a metric that will allow you to “answer” the measurement objectives. This could be a simple count metric (such as “number of critical vulnerabilities remediated last month within two weeks of discovery”) or a derived metric (such as a “percentage change in time to remediate critical vulnerabilities over a three-month period”).
- *Develop a measurement approach.* For each metric, figure out how you will source the data you need and how and when you will “take a measurement” against the metric.

For a new cybersecurity program, consider keeping these metrics at a programmatic level rather than diving too deep into practice or control-based metrics. In other words, use the measurement capability to prove you are getting things done, closing gaps, and doing so in the most efficient manner. Limit the number of metrics to key indicators that are both meaningful and simple at the same time. Trying to impress senior management, Board members, and other stakeholders with too much quantitative information at one time can be counterproductive.

Also, now is a good time to consider other ways to measure effectiveness. After the first 90 days, you should be focused on improving your risk estimation and quantification skills. Risk quantification gives you a way to express investments and program effectiveness in terms of quantitative risk avoidance. It allows you to cast your program in business terms that are easily understood by decision-makers—simply by expressing a risk event in quantitative terms relative to actions you’ve taken and investments you’ve made to reduce the probability of such events from occurring. This is a powerful skill set you’ll want to cultivate as you continue to grow in the job.

Review the incident response plan. Before you leave this sprint, there is one critical task you must complete if you have not already: review and revise the organization's incident response plan. If one does not exist, now is the time to start outlining and building one.

Not only does this activity continue to help you develop important organizational relationships and a culture of cybersecurity, but it is an important readiness activity that needs to be accomplished quickly. Your colleagues will expect you to take leadership if an attack occurs and guide the organization to success. Thus, even without a formal plan in place, now is the time to consider how you would execute if an incident occurred. If an existing plan is in place, get familiar with it and revise accordingly.

Second 30 Days: Artifacts

If you've worked diligently through the recommended actions in this sprint, the following are some of the artifacts you should have created or acquired:

FInal 30 Days: Objectives

The objectives of your final 30 days are to focus on refining the artifacts you've developed to date and begin to actualize your vision.

This is the implementation phase, and it jump-starts your transition from "planner" to "doer." In this sprint, you'll refine your strategy and plan and begin laying the foundation for accomplishments to come.

In this sprint, your objectives include

Final 30 Days: Recommended Actions

You've done as much as you can in scoping, designing, documenting, and establishing a program. Now, start to make progress on your vision. These final 30 days are critical because you'll be asserting your leadership of the cybersecurity program and establishing yourself as the trusted authority in the organization.

Give management a status report. It's time to give management some idea of the health of its ability to defend against cyber-attacks and to deal with the inevitable intrusion. In the first 60 days, you collected and created artifacts that provide you with sufficient information to form a professional opinion on where the organization stands. You should use this opportunity to tee up the current strengths and weaknesses of the organization as a backdrop to your cybersecurity strategy and plan—with emphasis on how you plan to close the gaps that pose a considerable risk.

At any point throughout your time building this new program, you may be required to give a Board-level briefing. Use this meeting as an opportunity to set the stage for the current state, the future vision, and the strategy and roadmap that you'll use to bridge the two. Be prepared to provide some characterization of the organization's threat environment and, in particular, the key threats to which your organization is most susceptible. You may also get an opportunity to discuss the cost-of-cybersecurity in the organization as you see it. Depending on your current status with the Board, this can be a tricky conversation, but it can be easily navigated by discussing the value of current investments, technical debt that you would like to reduce, and new investments that will provide payoff in terms of risk avoidance and improved user experiences. And be sure to put yourself in listening mode: Board members are not shy about telling you their requirements and expectations, so capture what you can and use it to support your vision as you move forward.

Establish a cybersecurity steering committee. To date, you've spent a lot of time heads-down analyzing and planning. But, getting back out into the organization—especially with key stakeholders—is where you'll reengage and begin the implementation process.

One of the best ways to bring key stakeholders back to the table is to create and convene a cybersecurity steering committee. This committee should include representatives that will both help you realize your vision and be key contributors to refining it and clearing trees where needed. Depending on the organization, this may include representatives from Legal, HR, Risk Management, IT, Engineering, and Procurement. Keep in mind that if you need to create and support multiple programs, including an operational technology-focused program, you may need additional steering committees that can focus on the specific and unique challenges in that area. This is especially true for operational technology, which might include not only various types of engineers but also construction personnel, field telecommunications, and facilities support.

Your steering committee is also an excellent proving ground for your strategy, plan, roadmap, and budget artifacts. If possible, establish the committee and get their input of your program before meeting in earnest with senior management and the Board. Not only will they give you much-needed advice but they may also have some key tips for managing up-–the-chain in your new organization.

Connect to your industry and segment. Understanding the unique and shared challenges in your organization's industry can open new doors of collaboration and coordination that you may need to call upon for enhanced threat intelligence, brainstorming on similar problems, and event handling and containment. It's never too soon to seek an active role in organizations that support these objectives.

In addition to making connections with the Department of Homeland Security's US-CERT and Cybersecurity and Infrastructure Security Agency (CISA), you should explore local collaborators, which might include local information sharing organizations and law enforcement. Where possible, membership and participation in industry organizations that may provide vital cybersecurity support resources is an important goal as it keeps you attuned not only to potential threats but also emerging requirements (and potential compliance obligations). In fact, you may have an opportunity to frame and contribute to the development of these requirements so that they ultimately bring value to your organization.

Finally, you should join and participate in an information sharing and analysis center (ISAC) that best fits your organization's main industry. ISACs are nonprofit organizations that act as information gathering and clearinghouses relative to your industry's cyber threats. You can not only obtain information by participating in these organizations, you can also provide vital information that may affect other member organizations. This is especially important since critical infrastructure operators are often tightly connected and integrated, so a community view of cybersecurity is important, especially when incidents occur that could propagate across geographic and digital boundaries.

Consider doing an asset-based risk assessment. Hopefully, at this point, you've already done (or at least commenced) program and practice-level assessments to understand the organization's current capabilities. At this point, however, it's wise to consider doing a risk-based assessment to better understand the level of organizational risk exposure. Not only will this help you begin the process of risk remediation (especially for risks deemed to be critical), but it will round out your strategy and plan by giving you real-world scenarios that your program must address.

Additionally, an asset-based risk assessment will help you get familiar with the organization's key assets, the business owners of these assets, and the degree to which they are potentially affected by external parties over whom you do not have direct control. This is also an important first step to understanding your third-party risk exposure, especially for critical data that may be stored, transmitted, and/or processed outside of your direct influence.

Understand your third-party risk exposure. Speaking of third-party risk, if your organization has extensive external connections (think "cloud" or anything-as-a-service), they become part of the threat surface you'll need to manage going forward. It's time to understand the extent to which this extended surface poses a risk to the organization and how you're going to manage that risk.

If your organization does not already have a third-party risk management program in place, now is the time to start exploring developing such a program. This will entail discussions with such collaborators as Legal and Procurement to determine how new vendors are vetted with respect to their cybersecurity controls and how potential risks of these relationships are identified and remediated. This is also a good time to start surveying the organization as to data assets that may be in the custodianship of external parties—either stored, transmitted to them, or processed by them. A comprehensive data inventory is key to ensuring proper controls over external handling of critical and regulated data are in place.

If third-party risk is a key challenge you'll need to manage with your emerging cybersecurity program, be sure to elevate your concerns as part of your discussions with senior management and the Board. Too often, the exposure to cybersecurity risk is limited to the controllable organizational boundaries, when in fact, third-party exposure may greatly eclipse it.

Perform next-level planning on key areas. There are certainly several foundational cybersecurity areas of practice that need to be cultivated and refined on which to build future success. These areas are non-negotiable in that they form the universally-accepted core elements of a cybersecurity program. While you have gathered information on these capabilities earlier in the program, in this sprint, you need to do detailed planning (areas of improvement, gaps, starting from scratch?)

Key areas to consider include:

- *Privileged access management.* The use of privileged credentials poses a considerable risk to your organization. Protecting these credentials and ensuring acceptable use is one of your key responsibilities. A thorough understanding of your organization's key capabilities in this area—policies, practices, tools—is necessary to ensure an appropriate balance with the administrative needs that accompany today's computing environments. Look for strong vaulting, logging, and auditing capabilities and identify gaps that you might want to address as a high priority.

- *Identity and access management*. Identity and access management is a gateway to ensuring acceptable use of organizational assets and supports the key objectives of least privilege and segregation of duties. Take a detailed look at how the organization manages identities and provisions and deprovisions access. Gaps in these processes might indicate excessive access privileges that pose a risk. And, don't forget to survey the degree to which access credentials have been provided to external parties. External users may be much less attentive to the proper use of the keys to your environment.
- *Vulnerability management.* Being able to remediate vulnerabilities quickly is a fundamental defensive activity. Longer times-to-remediate result in increased exposure to risk, particularly ransomware. Perform critical analysis on the vulnerability management process in the organization, including how vulnerabilities are identified, on what assets, and how quickly "critical" and "high" vulnerabilities are remediated. Look at the interplay between cybersecurity and IT management to ensure cooperation and collaboration on addressing vulnerabilities. Small changes in the vulnerability management process can have positive effects on the organization's risk profile, so look for some quick wins in this space.
- *Cyber Hygiene.* Preventative and maintenance hygiene on the organization's key assets—systems, networks, and data—is an investment in reducing risk and exposure. Preventing the use of potentially damaging tools and methods (such as local administrative privileges), failing to close unneeded communication ports or turning off services, or limiting the use of third-party software are all practices that can easily be implemented with significant payoff. Spend some time examining your organization's cyber hygiene approach and the current "health" of the computing infrastructure. There are numerous tools—some of which are free—that can help you quickly determine where insecure configurations exist and can be quickly fixed. A partnership with IT infrastructure management is critical here and can be a defining collaboration on which to build future efforts.

Score a few early wins. Nothing will help your future program build success and confidence with your leadership like achieving some quick accomplishments early in the program.

In your first 30-day sprint, you inventoried the organization's cybersecurity capabilities and became familiar with IT processes, architecture, and infrastructure. In the second 30-day sprint, you did a deeper dive by further assessing the organization's cybersecurity practices and controls and created a strawman roadmap of activities and projects that will define your program at a functional level for years to come. As you performed these actions, you documented areas of concern, perceived gaps, and improvement opportunities.

At this point, you have a fresh perspective of what is working in the organization and what isn't. And you can use this information to establish a set of quick wins: actions you can take and things you can do that require minimal investment (if any) but have a measurable impact on the organization. Using all you have learned to date, create a realistic list of these actions and projects, complete with time and resource estimates. Round out your list by documenting the value proposition to the organization. Decide whom you will have to get involved with to help and collaborate. Some easy wins might be revising (or drafting) the organization's cybersecurity policy or publishing (or revising) the organization's incident response plan. You might also find ways to help with existing stakeholder projects or put some energy in remediating high-impact/low-investment risks you identified in the asset-based risk assessment. In the end, the objective is to not only get something done but to demonstrate to the organization that cybersecurity can be a value-added activity.

Explore a cyber risk quantification approach. At its core, cybersecurity is one of many organizational risk management activities. As such, it lends itself to traditional risk management tools and methods that can give your program more credibility because it helps you translate technical constructs into language that business owners and decision-makers are familiar with.

A key emerging area of cybersecurity risk management is risk quantification. Put simply, risk quantification is the ability to express risk in quantitative or financial terms. In cybersecurity, risk quantification is often relegated to qualitative expressions such as "high" or "critical," but this is inadequate for decision-makers who often rely on bottom-line impact to prioritize investments. Building a capability for expressing cyber risk in a language that senior leaders can appreciate and act on is a key skillset for all CISOs.

Now is a good time to explore how your organization addresses risk quantification—what methods they use, how they report and use this information, and how it is incorporated into decision-making. There are many emerging risk quantification tools and methods specifically for cybersecurity that you should incorporate into your program. In the end, your ability to express cyber risk in quantitative terms may be the biggest catalyst for your program's future success.

Final 30 Days Artifacts

If you've worked diligently through the recommended actions in this sprint (and built on your accomplishments in the first 60 days), the following are some of the artifacts you should have created or acquired:

Congratulations: you made it through the critical first 90 days! This can be a stressful time for any new project, but your role as the cybersecurity leader is especially challenging. Not only do you need to understand the scope of your responsibilities, but you are expected to have all the answers when managing day-to-day cybersecurity.

As you look back on the first 90 days of this new program, do a detailed evaluation of where you stand. Being honest about this initial time period can help you make necessary corrections (if needed) while you're still building a robust approach to cybersecurity. And, if you need help, now is the time to get it.

Consider answering the following questions to evaluate your performance:

- Am I on track to meet the program mission, goals, and objectives? Do these artifacts need revision at this point?
- Do I have a viable strategy, plan, and roadmap? Is it realistic as to time, cost, and other resources?
- Do I have a working understanding of the organization, especially IT? What knowledge gaps exist, and how will I close them?
- What relationships are going to need additional work?
- What barriers and constraints have I identified over the first 90 days? Which ones can easily be overcome, and which need more consideration? Will any of these barriers and constraints derail progress and success, and why?
- Do I have a clear understanding of the current state of cybersecurity in the organization? Am I clear on the critical gaps and risks? Have I communicated effectively to management where the organization stands?
- Do I have a clear understanding of the expanded threat environment and scope due to third-party exposure? Have I engaged external partners to support my program?
- Have I made progress on demonstrating value through early wins and closing gaps in key areas?

Cyber governance

Describe the company's governance of cybersecurity risks as it relates to:

- The board's oversight of cybersecurity risk, including identification of any board committee or subcommittee responsible for oversight and the process by which they are informed about cyber risks.
- Management's role and expertise in assessing and managing material cybersecurity risk and implementing cybersecurity policies, procedures and strategies.
- Specific disclosure of any management positions or committees responsible for assessing and managing cyber risks, including discussion of their relevant expertise.

Just as Axio has designed its platform to assist Board members in making informed business decisions, the SEC's mission is to do so for investors. Its stated purpose is to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation," which aligns directly with the proposed amendment's goal to improve and standardize existing regulatory framework and reporting requirements around "material cybersecurity incidents" for public companies. Should it pass, the amendment is designed to give shareholders a better picture of the potential material impact of cybersecurity incidents on their investments.

Most Board members already know that cybersecurity should be managed from a business and financial standpoint, and Board coherency around cybersecurity risk from a financial impact perspective is no longer optional for a successful business. Yet, this regulation comes as a necessity. In its Public Company Governance Survey report, the NACD (National Association of Corporate Directors) found that 61% of directors said they would be "willing to compromise on cybersecurity to achieve business objectives." The NACD also noted that Board members would like to improve their effectiveness in "core oversight areas," including cybersecurity, yet over 70% believe that they already spend too much meeting time on the topic.

The NACD's findings are troublesome from a cybersecurity professional's standpoint, but with Axio's risk-based approach to cybersecurity, "cybersecurity and achieving business objectives" are one and the same, and boards can maximize the ROI of cybersecurity spending and the return on the time they spend puzzling over existing cybersecurity policies and procedures. The SEC specifically suggests that both qualitative and quantitative analysis are needed to assess the materiality of a cybersecurity incident. Axio's methodology and software can assist business leaders by presenting all the data required by the SEC's proposed amendment.

Axio has helped thousands of organizations benchmark, plan, and manage their cybersecurity, risk management, and risk quantification programs. Our work with organizations across several critical infrastructure sectors—such as health, energy, utilities, financial, and manufacturing—focuses on improving cybersecurity through a risk lens that organizations can use to facilitate better cyber-defense decisions and allocation of investments.

A cornerstone of our approach is the Axio360 platform. Through the Cyber Program Planning and Management capability, organizations can use the platform to quickly assess their cybersecurity programs and build improvement road maps aligned with common industry-accepted frameworks such as NIST CSF, C2M2, CIS20, and CMMC.

David W. White
President & Co-founder

David White leads Axio's innovation team and federal team and is actively involved with clients deploying the Axio360 software solution. He co-developed Axio's cyber risk management process and continues to refine the assessment, risk modeling, threat analysis, insurance analysis, and software solution that comprise that process. He has deployed the Axio360 solution with customers within the energy, utilities, financial, manufacturing, pharma, medical device, professional sports, and entertainment sectors. He served in a leadership role in the development of the Cybersecurity Capability Maturity Model (C2M2) versions 1 and 2 in support of the US Department of Energy and is a frequent speaker at board meetings, conferences, webinars, and other events. David co-authored the CERT Resilience Management Model (CERT-RMM) and was the chief architect for the Smart Grid Maturity Model (SGMM).

Richard Caralli
Cybersecurity Advisor

Richard Caralli is a senior cybersecurity advisor with significant executive-level experience in developing and leading cybersecurity and information technology organizations in academia, government, and industry. Caralli has 17 years of leadership experience in internal audit, cybersecurity, and IT in the natural gas industry, retiring in 2020 as the Senior Director – Cybersecurity at EQT/Equitrans. Previously, Caralli was the Technical Director of the Risk and Resilience program at Carnegie Mellon's Software Engineering Institute CERT Program, where he was the lead researcher and author of the CERT Resilience Management Model (CERT-RMM), providing a foundation for the Department of Energy's Cybersecurity Capability Maturity Model (C2M2) and the emerging Cybersecurity Maturity Model Certification (CMMC). During his 15 year tenure at Carnegie Mellon, Caralli was also involved in creating educational and internship programs for master's degree and continuing education students in the Heinz College.