How to Establish Your Vision and Gain Cybersecurity Traction

BARR ADVISORY

Table of Contents

3 Introduction

4 Establishing Your Cybersecurity Vision

6 Achieving Alignment

7 Gaining Traction

9 Measuring Your Traction

10 About BARR Advisory

Introduction

Having a vision of what you'd like to achieve is important for all strategic business priorities—and cybersecurity is no different. With a constantly evolving threat landscape, it is never too soon to evaluate the strengths and limitations of your organization's current cybersecurity program and to set a goal for an improved future state.

But just setting that vision isn't enough. Cybersecurity is more than just an exercise you can check the box on and forget about—it requires continuous improvement and consistent alignment throughout an organization. So once you've set that vision, how can you be sure you're gaining traction in your cybersecurity efforts?

In this whitepaper, we'll delve into how to establish your cybersecurity vision—but we won't stop there. You'll also learn how to gain traction on your cybersecurity efforts and continuously evolve your vision over time as your organization scales.

Establishing a Cybersecurity Vision

Establishing a cybersecurity vision, communicating that vision to everyone in your organization, and knowing your opportunities for improvement are what make positive change possible. Establishing your vision is powerful because it builds a culture of cybersecurity, helping the people in your organization understand their personal responsibility toward the shared vision.

Strategic Objectives

For most organizations, having a robust cybersecurity program that adds resilience and builds trust is part of the long-term vision. Establishing the right program can feel overwhelming, but no organization is too big or too small to establish and benefit from one. Making that vision come to life begins with understanding your current cybersecurity posture and outlining strategic objectives based on the gaps and weaknesses.

If you're struggling with where to begin, businesses can start by asking themselves:

- Have we selected a reliable framework on which we want to base our policies and controls?
- Have we performed a risk assessment?
- Do we have effective policies and controls in place to manage risk?
- Are there areas of improvement? Can we simplify controls to help us work smarter rather than harder?
- Are there controls we're doing manually today that could be strengthened through automation?
- Are there framework requirements that we haven't met because we're missing controls?
- Do we have the right people in our organization operating and maintaining our cybersecurity program?
- Do we have a culture that takes security seriously?

To create meaningful short and long-term objectives, start by assessing where your organization is today with a risk assessment. Find a well recognized framework for managing cybersecurity (such as the 18 CIS Controls, NIST, ISO 27001, or SOC 2) and review the framework requirements to determine whether or not you have controls in place to address the risk of each requirement. Any gaps in control coverage can be assessed to determine actionable next steps that will improve your cybersecurity program.

If your organization needs help with a risk assessment, consider virtual Chief Information Security Officer (vCISO) services that can provide guidance and expertise on how to improve a cybersecurity program, or get one off the ground.

If you're getting started on your journey, it's going to be important to get approved policies implemented and communicated to your organization. You'll want to train your personnel on cybersecurity trends and their personal responsibilities. Spread the word and create a culture of security-mindedness.

As you outline long-term goals, think about the potential certifications your organization may want to achieve. SOC 2 and ISO are excellent goals for many small to medium-sized businesses. Long-term goals should also be mindful of continuous improvement—consistently asking where your organization can improve controls or scale processes.

Frameworks for Managing Cybersecurity

- 18 CIS Controls
- NIST
- ISO 27001
- SOC 2

Achieving Alignment

Gone are the days that cybersecurity is siloed somewhere within the IT department. Cybersecurity should be a strategic priority for any modern business and needs to be discussed at the highest level of the organization alongside other business priorities such as customer satisfaction or growth.

Simply having a vision and communicating that vision is the first step to aligning your organization with shared cybersecurity goals. When people understand where their organization is headed, they can do their best to work to figure out how to get there without wasting energy going in multiple directions or wondering how their work makes an impact.

Here are a few communication strategies to help your organization get and stay aligned:

- Set and communicate your vision.
- Hold everyone accountable with defined, actionable, and measurable tasks.
- Keep cascading messages simple.
- Say important things multiple times.

It may take some time to get everyone on the same page, but the results can be exponential. Now that we've covered how to establish a cybersecurity vision, let's learn more about how to gain traction with your organization's alignment, processes, and people.

Gaining Traction

Oftentimes the idea of cybersecurity can be overwhelming, particularly for smaller businesses that aren't sure where to start. Small steps like staying up-to-date with industry blogs and webinars, attending trainings, and communicating common themes you've noticed across your organization are excellent ways to begin gaining traction in your cybersecurity efforts and achieving continuous improvement. Once security is ingrained across the organization, then you can begin to think about cybersecurity certifications or aiming for a SOC 2 report. It can be helpful to have someone, or a group of people, that are designated as security leaders within the organization to keep everyone on track.

Gaining Traction with Alignment

Organizational alignment on a cybersecurity vision with short and long-term goals is crucial. Once you've established your cybersecurity vision, it's important to measure and track how your organization is gaining traction toward its goals.

If you've already performed a risk assessment, establish a regular cadence of meetings to make sure everyone from leadership down is on the same page with cybersecurity initiatives. Use the risk assessment as the leading point for the agenda for these meetings —after you've identified security-related risks, you can create action items to remediate those risks. A key part of these regular meetings is to follow up on action items and provide status updates to key stakeholders. These meetings can also provide an opportunity to discuss any issues or potential issues. Depending on your organization, these meetings can be held quarterly or even monthly.

Regular security-focused meetings can also be used to keep everyone up-to-date on the latest cybersecurity trends or breaches. One strategy is to use security meetings as a book club—everyone reads a book, article, blog, or listens to a podcast prior to the meeting about a relevant cyber trend. Part of the meeting can be dedicated to discussing what they learned and how it may affect their organization.

If your organization is working towards any certifications or reports, these meetings are a good time to have regular internal updates on the progress.

Gaining Traction with Cybersecurity Processes

The most important thing organizations can do to gain traction on their cybersecurity processes is to prioritize security from the very beginning. Whether it's a new process or a new product, it's much easier to implement security measures early on instead of going back later.

Having an automation-first mindset can also help you to continuously improve your processes. Ideas can naturally flow when you determine what manual activities can be automated so that you can focus more fully on the real prize: security.

It's also important to stay on top of ongoing trends with industry certifications. There are always new certifications or refreshes to existing ones. Instead of just working towards a SOC 2 and stopping there, continue looking for ways to improve your security by researching and identifying the framework that works best for your organization.

Gaining Traction with People

Most organizations have an annual security awareness training, which is important, but it's just as important to think about your people from an ongoing perspective. It's easy for the security mindset to go stale if employees only need to think about security once a year. Regular, company-wide communication about security efforts or book clubs across different departments are helpful for keeping cybersecurity top of mind.

When you hone in on the importance of cybersecurity and employees buy into it, they're more likely to naturally think about baking cybersecurity into their processes instead of waiting to be told to do so. Too often, company culture makes employees worried they'll "get in trouble" for failing a phishing test or security training. When organizations prioritize security and the role everyone plays in the organization's cybersecurity objectives, it can help employees get on board. Building a cybersecurity culture helps with ongoing, continuous improvement when it comes to your organization's employees.

Measuring Your Traction

Cybersecurity efforts need to be continuously measured. It's not enough to simply set your goals—progress needs to be tracked in order to continue guiding your organization in the right direction. A cybersecurity scorecard is an extremely valuable tool for measuring your organization's traction toward the cybersecurity vision. A scorecard is an evaluation tool that provides a quantified measurable against a predetermined key performance indicator (KPI). You can learn more about how to set cybersecurity KPIs and implement a cybersecurity scorecard with BARR Advisory's How To Use Cybersecurity KPIs whitepaper.

When the mindset of continuous improvement is part of the cybersecurity vision and culture, it gives your organization the opportunity to grow, become more agile, and achieve cyber resilience.

About BARR Advisory

At BARR Advisory, we build trust through cyber resilience. We help protect the world's data, people, and information networks through a human-first approach to cybersecurity and compliance. Businesses looking for the accessibility of a boutique firm with the tools and expertise of a global consulting firm will find a partner in us.

Specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud, BARR has the global network of partners, the perspective, and deep expertise every thriving SaaS provider to world-class enterprise needs to stay secure and compliant at every stage.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/ HITRUST]
- **ISO 27001 and 27701 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Virtual CISO Services**
- **People & Culture Services**

Connect with BARR

Want to learn more about the role of the CISO or if your organization could benefit from a virtual CISO? Contact us today.