CHAPTER 10

Obtain Buy-In from Stakeholders

We'll Cover

- The concept of buy-in and why it's needed for the success of a security metrics project
- How to prepare for a buy-in meeting with stakeholders
- A step-by-step process for obtaining buy-in for a security metrics project

A big mistake that some security professionals make is not engaging stakeholders early enough and, therefore, failing to obtain stakeholder buy-in for security metrics projects. This applies in general to many security projects, but because this book is about security metrics specifically, here I will discuss the importance of obtaining stakeholder buy-in and their commitment to timelines for security metrics projects.

What Is Buy-In and Why Do You Need It?

Most security metrics projects cannot be done in a vacuum using only resources, budget, and time from the security team. Due to the comprehensive nature of information security and the capability of today's technology to store, transfer, and retrieve information in so many different formats and in so many different places, we as information security professionals are often faced with situations in which we need support from other teams to achieve our objectives. Obtaining buy-in involves first identifying all of the different stakeholders whose support is required for a security metrics project to be successful and then ensuring that they understand the goals of the project and are committed to achieving them. A security metrics project may have only one stakeholder but typically has several. When identifying stakeholders, it is important to note their roles and responsibilities, such as owners and end users of systems or facilities involved in the security metrics project, audit team members, and so forth.

The information security team's job is to protect the information assets of the organization or company. An information security program is most effective if it aligns with business strategy by ensuring that the security metrics projects are adding value and that the value is clear to stakeholders and sponsors.

IMHO

Sales and communications are not necessarily the first skills that come to mind when thinking about the traits required for an effective information security team; however, both of these skills will play a role in any job you take as an information security professional. Information security is an area where expertise can be very specialized, and conveying the value and the "why" of security metrics projects to sponsors and stakeholders is not always straightforward or easy to do.

What happens if you don't have buy-in from your stakeholders? Too often, security metrics projects are set up for failure because buy-in is not obtained before it's needed. By the time stakeholders are properly identified and looped in, they don't have time to participate in the project or don't consider it a priority.

If stakeholders don't understand the "why" behind security metrics projects and aren't committed to achieving the same goals as the security team, then security metrics projects that need help from IT, operations, or any other supporting team may continue to be deprioritized (and won't get done) quarter after quarter.

Tip

Security will not be embraced by all, so buy-in is most necessary at the highest levels of stakeholders and not always necessary with the end-user community. Focusing on the highest-level stakeholders and obtaining their buy-in can give you leverage over lower-level stakeholders who might not be as willing to embrace the project.

Preparing for a Buy-In Discussion with Stakeholders

In this section, I describe "the homework" you'll need to do as you prepare for a meeting with stakeholders. You may get only one or a few chances to sell your security metrics project. The best way to approach this conversation is to have a comprehensive understanding of both what you're trying to communicate and what will work best for your particular audience.

Understanding Your Part

The first thing to do before approaching stakeholders is to understand what you are doing and what you will need.

What Are You Doing?

To obtain stakeholder buy-in and get your stakeholders to commit to timelines, you must be clear and convincing when you make your presentation. This requires that you have a solid understanding of what you're trying to achieve through your security metrics project. If you've read the previous chapters in this book, you should be well prepared. In Chapter 7 you learned how to define your goals and objectives, which should help you to explain to stakeholders the "why" behind your security initiative. Chapter 8 explained how to prioritize your security initiative within the context of both information security and overall company priorities, providing you with solid arguments for why this project is important to the company and why now is the right time to do it. Chapter 4 provided

you with the necessary business justification and project proposal framework to answer most of the questions that you may encounter as you begin your selling journey. All of this upfront work will come in very handy when you're selling the project to your stakeholders.

To help you organize your presentation of what you're trying to achieve through your security metrics project, here's a summary of the things you've developed in previous chapters that you'll want to have available for review as you're preparing to obtain stakeholder buy-in:

Chapter 4	Brief Objective Statement Type of Change Proposed Start and End Date Roles and Responsibilities Project Name Problem Statement Solution Statement Priority/Principle Supported Scope Project Description Change Details and Impacts Risks of Not Implementing This Project Dependencies Metrics/Success Measures Major Deliverables and Deadlines Required Budget Resources Required
Chapter 6	Target
Chapter 7	Objectives/Goals
Chapter 8	Priorities
Chapter 9	Key Messages

With your homework done, you're ready to provide a clear agenda for the discussion with your stakeholders. During the actual meeting, I recommend presenting the information in the following order:

1. Key Messages
2. Problem Statement and Solution Statement
3. Target
4. Objectives/Goals

You can then follow this discussion with a more detailed presentation of the project plan components from Chapter 4.

Into Action

You also have requirements for the project, and depending on the role that the stakeholder team plays, they may have requirements too. You'll need to discuss both.

First you'll need to lay your requirements out on the table with regard to resources, budgets, and timelines. If you're pursuing a project with stringent deadlines and deliverables, such as a compliance remediation that is needed to pass regulatory requirements, then you will need to take a hard approach where you state what absolutely must be done and what you need to accomplish it. Because the project is mandatory, you should not meet stakeholder resistance to your requests. Your task, then, will be to work with the stakeholder teams to figure out the best way to meet those requirements. On the other hand, if you're proposing a project that is not mandatory, you'll have to take a more delicate approach when you lay out your requests, and then work within the means of your stakeholder to get what you need. Without the compliance requirements of the first example, you'll need to convince your stakeholder that your project is enough of a priority to dedicate the required resources and budget.

If the stakeholder team that you're meeting with is a customer of the security team, you'll need to obtain their requirements to ensure that your team delivers what they need according to their specifications. This meeting is the perfect place to do so, and you can use the project proposal/business justification form in Table 4-1 of Chapter 4 as a guiding document to facilitate the discussion.

What Do You Need?

The second step in preparing your presentation to obtain stakeholder buy-in is to identify your potential stakeholders and sponsors.

Access Sometimes, to accomplish your objective, the only thing you need from a particular stakeholder team is access to their systems. Your information security team may have the bandwidth and the expertise to do the work that needs to be done, but you may need to request and gain access to certain systems or applications to get the job done. Your work may change or impact the systems and applications that you're accessing, in which case you'll need to request from the stakeholder team the access and permissions to make the changes.

Resourcing and Budget The two biggest things that you will likely be requesting from your stakeholders to accomplish your objectives are their resources (specialized expertise and work from their team members) and their budget for hardware, software, consulting, or maintenance costs to support your project objectives.

Outline your requirements first and then ask the stakeholder team to define the specific resourcing required. You are the security expert and they are the expert in their field, so when it comes to allocating their resources and how much time it takes for things to get done, they know best. Similarly, if you're putting forth security requirements for a big technology purchase that will be chosen and deployed by the stakeholder team, it's best to center the discussion on security requirements rather than prescribing pieces of the project, which is their area of expertise.

IMHO

It's important when talking about resourcing and budget to communicate your requirements to the stakeholder team and then ask them for the resource and budget estimates. It is critical to ask how much it will take rather than specifying it yourself—with this approach you're more likely to get something closer to what it will actually take as they know the historical data best. Additionally, you're protected against blame for scope issues down the road.

Timelines One of the critical things for which you need stakeholder buy-in is the timeline for your project, particularly regarding the phases during which the stakeholder teams will need to perform work, grant access, or have their systems affected by other work involved in the project. Timing is one of those project management components that may or may not be flexible, depending on the project needs and situation. For example, an audit project that has a tight deadline will have very strict timeline requirements, and to meet those requirements, other project parameters such as budget and resources must adapt to the timeline. On the other hand, another project may exist that has limited budget and resources but is more flexible in terms of the timeline. In that case, the project may ration its budget and resources over time to deliver the project successfully.

Tip

If you have a rigid timeline, communicate that fact to the stakeholder team and explain why time is of the essence. If you have a flexible timeline, begin by outlining your requirements and then ask the stakeholder team what they estimate for resourcing needs.

Understanding Your Stakeholders

As discussed in Chapter 9, you need to understand your stakeholders prior to meeting with them. Make sure you have as much information as you can gather beforehand regarding what they're responsible for, what they care about, what they're working on, and the history between your team and theirs.

LINGO
A **pain point** is exactly what it *sounds* like—a problem that has been particularly difficult to solve.

Why is it important to understand the history between the teams? Understanding past relationships and events that have occurred can give you insight into both what's worked and what hasn't worked and help you to shape your presentation accordingly. Success stories can provide a context to which you can refer as you present your current case for a new security metrics project, and pain points and conflicts from the past can guide you in formulating a new approach.

As an example of why it's important to understand the history between the teams, suppose your team previously initiated a secure coding training project for developers that resulted in fewer application vulnerabilities on the corporate website and, consequently, more time for the developers to work on other issues (instead of fixing vulnerabilities and taking the heat for any that might have been exploited). The next time you approach the development team with a security idea or a new project, they're likely going to listen to you as a trusted authority. If, however, your team previously deployed onto the corporate network a monitoring tool that ended up breaking business-dependent systems and

Into Action

In addition to the resources listed in the table in "What Are You Doing?" here are some guiding questions that you can use to identify which teams you'll need buy-in from:

- Which teams will need to provide support?
- From which teams will you need resources and time to make your project happen?
- Which teams will be affected during the implementation and rollout of your project?
- Which teams will need to be informed about the project deployment and results?
- Which teams are the customers to whom you will be providing services?

Into Action

Discuss success stories in a quantitative manner by including details about the number of hours, dollars, and headcount involved in the past projects. Also, recruit an advocate within the group of stakeholders prior to the meeting, to help keep the meeting on track and continuously refer to past successes. Finally, address past negativity up front. Let your stakeholders know that you understand their pain points and that your team will avoid past mistakes or obstacles to ensure the success of the project.

causing downtime, then the next time you approach the IT team with a request to evaluate or implement more security tools on the network, you're going to have a tougher time convincing them. You will need to research the new tool and present information to the IT team that convinces them the new tool is not going to interfere with their systems and customer needs.

Finally, when deciding whom to include in your meeting with a stakeholder team, there are two different roles to consider: the decision-maker and the worker.

Including the decision-maker ensures that the person who is responsible for allocating resources and making approval decisions is present. Getting that person to understand why your project is valuable and is a priority is often very important to obtaining buy-in. The downside is that, depending on the level of the decision-maker, that person may lack the specialized expertise to know exactly how long something will take or to give you insight into additional specifics, risks, and issues related to the "how."

The advantage of including the worker who will be performing the actual tasks is that they will know all about the "how," including technical intricacies, specific historical information about what has worked and what hasn't in the past, and the different players who will need to be involved to get the job done. It will be important for you to specify your requirements to the team members in this role so that they know what to do. They will most likely be able to provide more accurate input than the decision-maker in terms of scope and what additional resources outside of their team may be required. The disadvantage is that they may not hold the decision-making power required to utilize their time (even if they think that your project is a great idea, their boss may have them working on something deemed to be a higher priority).

My recommendation is to include both of these types of stakeholders in your meeting, if possible. If not, start with the folks in the worker role to get an accurate scoping, and

In Actual Practice

How do you learn about the history between the teams? If you have a senior security team member who has been around for a long time, you might be able to simply ask them, either during a casual conversation or a quick meeting that you set up specifically for that purpose. If you know someone within the stakeholder team that you are trying to engage who might be able to provide insight into what's happened in the past and how the relationship between the two teams works, then you might want to consider reaching out to them as well prior to kicking off your stakeholder buy-in meeting.

If no one on the security team has been around long enough and you don't have contacts on the stakeholder team, consider reaching out to vendor contacts who have been doing business with your company for some time. Often, security vendor partners or resellers also have relationships with IT and network operations teams, and if the vendor is well established and has been doing business with different groups in your company for some time, then they may be able to provide you with some information.

then follow up with the folks in the decision-making role in order to get final buy-in and management approval. Getting stakeholder buy-in from only one or the other may lead to unnecessary friction and project hold-ups down the line.

Tip

None of this "soft research" is intended to dictate your specific actions or approach; rather, it's just good information to have when going in to ask for stakeholder help on a project.

The Steering Committee

If multiple stakeholders are involved in a single project, program, or initiative, a steering committee type of format may be best. A steering committee typically consists of decision-makers from various teams (although other formats include workers, or perhaps two separate but related committees of decision-makers and workers). This type of group may meet on a monthly or quarterly basis to guide and direct major company initiatives, ensure that initiatives are aligned with organizational growth and drive competitiveness,

ensure alignment with industry best practices and standards, and provide a forum for reviewing, discussing, and approval project requirements, scope, priorities, and resource allocations. A steering committee may be focused on a particular aspect of the company or organization, such as risk management or technology.

If a steering committee whose charter is relevant to your security metrics project exists, you may want to present your project proposal to that committee for their discussion and approval. If one does not exist, you may want to consider creating one for the purposes of meeting the objectives previously described. This type of committee can evaluate and prioritize project proposals, determine prioritization, scope, and resource allocations, and follow up on ongoing projects to check their progress and calibrate prioritization against other existing and new projects.

Meeting, Explaining, Asking, Documenting

After you have prepared to meet with stakeholders by identifying what you're trying to achieve through your security metrics project, identifying what you need to request from stakeholders, and gathering as much information as you can about your stakeholder group, it's time to meet with them. This section addresses what you'll need to discuss with your stakeholders and get their input on.

As discussed, the first thing to present to your stakeholders is a description of what you're trying to achieve through your security metrics project. The second part of the presentation is an explanation of what you need. It's important to note that the second stage should be a two-way conversation: while you're specifying what you need, you must also find out what the stakeholders can provide, to ensure that the teams are aligned.

Documentation and Commitment

After you've outlined your project proposal and requirements and your stakeholder has filled in the gaps, make sure that you ask specifically for the stakeholder team's commitment to what's been estimated in terms of resources and timelines. Ensure that this buy-in is also documented in meeting minutes. You can then easily distribute the minutes via e-mail to make the information available to anyone who was not present in the meeting. More importantly, you can refer to this documentation as the project progresses in order to ensure that the stakeholder teams follow through with their commitment as things change and priorities shift. When the project is underway and questions arise, you'll already have the answers, and these will be transparent and already agreed to. Think of it as a security contract, and use it as such.

Note

After you've obtained and documented stakeholder buy-in and launched your project, don't forget to follow up with your stakeholders on a regular basis, communicating the project status and ensuring that commitments are being followed. You can also communicate project accomplishments, risks, and issues on a weekly, biweekly, or monthly basis. This topic will be discussed further in Chapter 13.

We've Covered

The concept of buy-in and why it's needed for the success of a security metrics project

- Most security metrics projects cannot be done in a vacuum using only resources, budget, and time from the security team.
- Obtaining buy-in involves first identifying all of the different stakeholders whose support is required for a security metrics project to be successful and then ensuring that they understand the goals of the project and are committed to achieving them

How to prepare for a buy-in meeting with stakeholders

- Organize your presentation.
- Make sure your description of what you're trying to accomplish and what you need from stakeholders is very clear.
- Make sure you've done your homework on your stakeholders—who they are and what they need.

A step-by-step process for obtaining buy-in for a security metrics project

- The key steps to obtaining buy-in are understand what you are doing, understand what you need, and understand your audience.