Chapter 3
Developing Your Information Security Program

A multibillion-dollar international company found that the email of an executive based in Germany was being regularly disclosed outside the company in an unauthorized manner. The investigation was complicated. The company's corporate headquarters was in the United States, so the investigation was based there because of the extremely sensitive nature of the incident. However, the executive in question was a German citizen, the mail server used by European-based executives was in France, and the breach appeared to originate at a Dutch facility.

Who had jurisdiction? Local law enforcement in the state of California, where the company was headquartered? Federal law enforcement in the United States? The Federal Bureau of Investigation (FBI) or the Secret Service (USSS)? French law enforcement because the email server was physically located in France? German law enforcement because one of its citizens was the target? Or Dutch law enforcement because the breach appeared to originate in Holland?

What laws and regulations are investigators expected to follow? Because this issue involves personal privacy, does company policy based on United States laws prevail? Or does German law on employee privacy prevail because the target was a German citizen?

Information security can be complex and requires a consistent methodology to ensure that the program remains current with threats and changes in laws and regulations. These changes occur at a rapid pace and are not consistent across different countries and industries. This chapter reviews a methodology that can be used to develop your program and account for these changes on an ongoing basis.

Introduction

The previous chapter introduced the key components of an information security program and the principle of *defense-in-depth*. This chapter introduces the core concepts that you should consider when building a new security program or improving an existing one. Both of these tasks require a solid plan and diligent attention to details. Using the methodologies introduced in this chapter, you can begin to create that plan.

When developing your information security program, you should begin by determining the high-level business objectives that you want to achieve. These objectives will serve as boundaries for the program and will guide your progress. By following a consistent methodology, you will be able to evaluate multiple alternatives and complete the design of your program.

The concepts introduced in this chapter will continue to serve you after you have a program in place. Changing circumstances will confront you with new threats and challenges, requiring you to adjust your program over time. Revisiting these ideas will aid you when making these adjustments and continually improving your program.

Overview

Developing and maintaining an information security strategy is essential to the success of your program. This strategy serves as the roadmap for establishing your program and adapting it to future challenges. By following a consistent methodology for developing your strategy, you are more likely to achieve high-quality results during the process and complete the project in a timely manner.

In addition, it is important to communicate the strategy and the processes that your organization will follow in simple terms that your non-technical staff will understand. As Chapter 2, "Information Security Overview" mentions, the success of any security program relies on the active participation of all personnel and their compliance with established security policies. By explaining all the policies and processes clearly and with minimal technical and business jargon, you increase the likelihood that your program will succeed.

This chapter aids you in evaluating your information security program and assists you in implementing an improvement plan that is appropriate for your company. We begin with a review of a methodology that you can use to guide the process. You can complete this process in a short period—as little as 90 days for most organizations—and by doing so, you will produce a 2-year roadmap for continually improving your program. Because the information security field is rapidly changing, you should review and update this roadmap on an annual basis because major revisions might be necessary.

Information Security Methodology

The information security life cycle illustrated in Figure 3-1 offers a broad overview to managing an effective information security program.

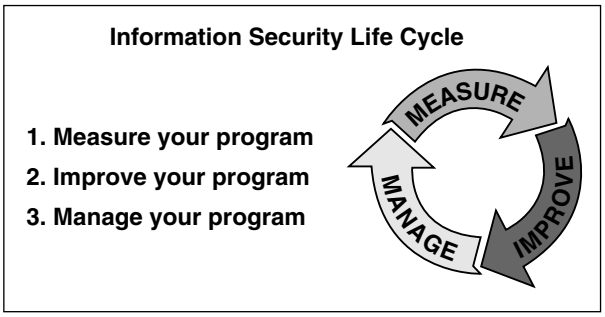

Figure 3-1 The information security life cycle.

The first step is to complete a thorough review of the current state of your information security program, which is referred to as a *baseline assessment*. This review will assist you in developing the plan for improving your program in the future.

After you have completed the baseline assessment, you are in the position to begin the second step in the process—making improvements. Evaluate the risks that currently exist in your environment and develop remediation plans to address them. You will need to prioritize these risks and address them in a balanced fashion over the course of the year.

Managing your security program is the third step in the process. During normal operations and while you are making strategic improvements to your environment, you will still need to respond to tactical issues. Remember, things change on a daily basis, and you will need to continually reevaluate your priorities for improving the program.

The circular nature of Figure 3-1 corresponds to the need for repeating the process over time. The next section introduces a more detailed methodology for accomplishing this.

Formal Information Security Program

Executives commonly ask, "How well are we protected, and what should we be doing to improve our program?" A recent security-related event inside an organization or a heightened awareness of security in general can prompt this question. Regardless of the reasons for starting a formal program, you should follow a structured methodology to guide your program. Although this is true in any critical business process, it's especially important in information security. By following a structured methodology, you can obtain results that are more predictable.

A structured methodology is similar to a therapy regimen prescribed by your doctor when recovering from an illness or accident. In this case, the illness might be a non-existent or weak information security program, and an accident might equate to an information security incident.

You should first step back and determine the business objectives that you want to support with your information security program. Evaluate the effectiveness of your existing program and determine where you would like it to be in the future. Aligning your security policies closely with your business strategy enables your company to achieve its objectives without hindrance because your staff is less likely to circumvent security measures that seriously impede them from achieving your core business goals.

The next step is the *gap analysis*—comparing where you are to where you want to be and examining the alternative methods to achieving those objectives. The investment you are willing to make in your program will determine its extent and the time necessary to put it in place. Again, keep in mind that this is a continuous process and you will need to update your information

security program as your business environment changes. Figure 3-2 illustrates a high-level methodology for evaluating your information security program.

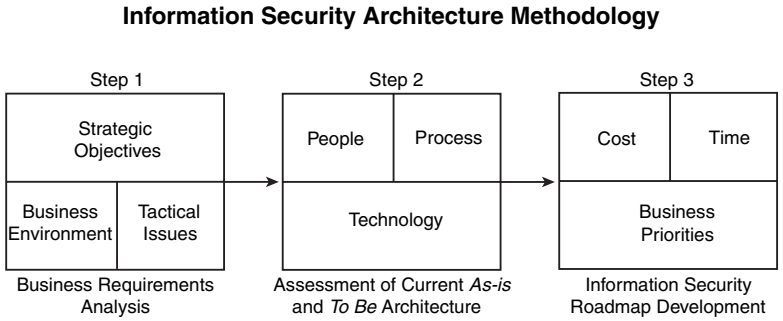

Figure 3-2 Information security architecture methodology.

Now we will examine each step in detail.

Step 1

The initial step in the process is determining the future business requirements that the information security strategy will have to support. The majority of this analysis consists of evaluating the three major areas through interviews with key managers within the company.

Strategic Objectives

- What are the company's long-term strategic goals?
- What are the major initiatives over the next 12 to 18 months?
- What are the information security requirements to meet these objectives?

Business Environment

- What is the company's line of business?
- What changes are expected in this industry over the next couple of years?
- What unique information security challenges or opportunities exist?
- How are other companies in your industry addressing information security, and which strategies have been successful?

Tactical Issues

- What information security issues currently exist that require immediate action?
- How do these issues affect the business?
- When must management address these issues?

Because it is important that your information security program supports rather than hinders your company from achieving its business goals, the results of this step necessarily form the broad boundaries for your program.

Step 2

Next, you evaluate the major components of your information security program to establish its current state and determine your goals for the program in the future. The components fall into three major categories: people, processes, and technology (the basis of your architecture). These are essential ingredients for an effective program (as we discussed in Chapter 2).

When assessing the current information security architecture, the objective is to become familiar with the existing environment, understand the current issues, and plan the future environment. This is not an exhaustive documentation of your existing environment; that level of detail is not required, and frankly, it wastes a lot of time. Some of the questions that you need to answer during this step are as follows:

- Does my organization have a formal information security strategy?
- How well has the program protected my company over the past year?
- Are metrics in place to measure the effectiveness of the program?
- Has the program undergone an independent review recently?

After establishing the current state of your program, you can begin to evaluate the possibilities for the future security environment, based upon the company's business environment and needs. The initial analysis should be broad and unconstrained because the goal is to define a long-term plan that you can tailor to what your company ultimately decides to invest in this area.

Some examples of the future environment include the following:

- A formalized organization that is responsible for information security
- Outsourcing selected portions of the program to vendors that specialize in these areas
- Upgrading your e-commerce presence to address potential security risks
- A company-wide security-awareness training program

You will use these results (that is, your gap analysis) in the final step to develop your future information security program.

Step 3

The major activities in this final step include the most important step in the process: leveraging the gap analysis between the current and future states of your program that form the foundation for the next steps required to define the roadmap. You need to develop a list of possible investment alternatives, along with the advantages and disadvantages of each one. The gaps that can exist within your program include the following:

- Your existing information security organization is not capable of managing the program
- Your company is not in compliance with industry regulations for information security
- Several high-risk areas exist within critical components of your business

Finally, you will provide the management team with alternative approaches for transforming the information security program. To make your case effectively, you must present these alternatives in business terms and specifically address how they will enable the company to accomplish the following:

- Increase revenue, improve staff productivity, and improve customer satisfaction
- Address industry compliance regarding security
- Protect company image and brand

Be clear regarding the specifics for each alternative you are proposing, how much they will cost, and how long it will take to deliver each recommended alternative. It is a good idea to circulate these alternatives within the management team during the course of your analysis, as opposed to waiting until the end to test their acceptance. Some of the changes you propose might not be readily accepted or might cost more than your company is willing to invest in information security.

Security Evaluation Framework

"How effective is our information security program?" is one of the most difficult questions to answer. Each business will judge success upon different criteria, depending on its industry and goals. A small mining company that only conducts business domestically and has few automated processes will require a different information security program from a large financial services organization that is heavily regulated and that conducts a considerable amount of business on the Internet. When evaluating these organizations, you must take into account the unique considerations of each business and industry best practices for information security.

The security evaluation framework outlined in this book includes 50 industry best practices for information security that were culled from multiple sources and presents you with a consistent methodology for grading your program. These best practices include people, processes, and technology categories. Scorecards have been developed to evaluate this component of your program. You can grade each practice area using three-tiered scoring as follows:

- "0" indicating the practice is not being followed at the company
- "1" for partial implementation of a best practice
- "2" for full implementation

The total possible score is 100 for a company that has fully implemented all 50 of the best practices. Use the results of your scores to pinpoint areas for improvement in your information security program. Identifying these areas is essential for developing your two-year improvement plan and is more important than the absolute score.

Unique company and industry characteristics are also important when evaluating your information security program because companies will vary considerably in their reliance upon security. The small mining company mentioned previously would have a low dependency upon information security, whereas security would be critical for a financial services company's operations.

The business dependency matrix (Table 3-1), which appears later in this chapter, identifies 12 critical characteristics for rating your company's dependency upon information security. By rating each characteristic as high, medium, or low importance, you can develop an understanding of how important an effective information security program is for your company.

Finally, by comparing the results of your program evaluation with your company's dependency upon information security, you can obtain a general idea of the effectiveness of your program. High-level guidelines are provided that you can use when determining the appropriate level of funding for your security program.

Conducting the Baseline Evaluation

The guidelines in this chapter offer a top-level view of the process that you should follow when evaluating your existing information security program or planning your future program. If you have not conducted an assessment in the past, you might consider bringing in an experienced third party to assist in this process. A third party will have methodologies to support evaluation and can train your staff to conduct future baselines. You should require that a third party uses industry standards rather than proprietary methodologies so that your organization can use the work it completes in the future.

Remember that this is just the first step in the process and that you need to move to your remediation step quickly to improve your security profile. Security programs can take considerable time to implement; for this reason, you should complete the evaluation as quickly as possible. You should be able to complete the methodology outlined in this book in 90 days.

Pulling It All Together

You will summarize the results of your analysis in a strategic plan that you will use as the roadmap for the next two years. Normally, one or more of the major program areas will have serious issues that you must address. It is important to start with high-level diagrams to convey your ideas and follow those with additional levels of detail. You'll find this is easier and more effective when you are presenting the plan to key individuals within the company.

You must provide management with a list of alternatives for migrating to the future information security environment along with the costs, timeframes, and benefits of each. Remember to present the recommendations in business terms and address how the program will affect revenue, staff productivity, and customer satisfaction. You'll need to test your recommendations to determine management acceptance during this timeframe.

The information security architecture document should contain the following information:

- Summary of the process used to develop the architecture
- Alternative solutions and recommendations
- Roadmap for implementation

Guidelines for developing the document include the following:

- Highly graphical
- Executive summary of 1–2 pages
- Main body of document that is 25 pages or less
- Bold recommendations because this is a great opportunity to make sweeping changes

The final information security architecture must address critical business objectives and be understandable to non-technical management. An effective approach is to find the optimal balance of addressing pressing tactical issues while also achieving the long-term strategies for the program.

Critical Success Factors

Management involvement during this process is important; management must consider information security a component of the overall business strategy for it to be effective. Otherwise, security will become just another initiative that is competing for management's attention and for limited company resources. Implementing an effective information security program will change how the company conducts business in the future, so clear communication of the process is critical. Employees need to understand these changes and the importance of information security in their organization's operations.

Another point to consider when developing your information security architecture is to set realistic expectations and not to over-commit. The costs associated with your recommendations could be significant and might require board of director approval. You must set goals that you are able to accomplish in an aggressive but achievable timeframe.

Information Security Methodology Wrap-Up

In 90 days, you can evaluate your organization's information security program and set the company on course for implementing future improvements. This requires a careful balancing act between addressing pressing tactical issues and making progress toward accomplishing strategic goals. By following a consistent methodology, you can clearly communicate to the organization the process that you will follow, get things on track, and start making visible progress.

It is important to follow a consistent methodology when establishing your information security program. The natural tendency is to look for immediate improvements when something goes wrong. However, this is a tactical rather than strategic approach, which isn't viable for establishing an effective information security program.

The methodology presented here provides an effective framework that you can easily scale according to the size and complexity of your business. The remaining portion of this chapter will cover the initial step of this methodology in more detail and provide examples of how you can use it at your company.

Business Requirements Analysis—Step 1 of 3

Follow the methodology introduced in the previous section to guide the development of your program. This includes first evaluating your unique business requirements to form the boundaries of the information security program. Major areas that you will evaluate include the strategic objectives for your program, your company's business environment, and tactical issues that you need to address immediately.

As we have emphasized, people, processes, and technology are the major components of an information security program. It is important that you carefully balance these areas because it is easy to focus on a single area such as technology and overlook other important components. Company size and complexity, risks, and unique business factors will define your individual program. A pragmatic approach to evaluating each area is outlined in the following sections.

Strategic Objectives

You can only establish specific security goals after you have clearly articulated strategic business objectives. You need to understand the real security risks and vulnerabilities that your business faces every day. Executives need to work together with the leader of their information security program to establish the company's long-term security objectives. This approach forces the company to think about security at an appropriately high conceptual level.

One example of a strategic objective for your information security program would be the appropriate handling of customer information. Companies now conduct much more business electronically, and their customers trust them with their confidential information. Unless the necessary controls are in place to secure this information, it is possible for dishonest individuals to steal personal information such as credit card numbers and make unauthorized purchases.

Balancing time to market and security is another objective for companies to consider for their information security program. Businesses today are under tremendous pressure to offer new products and services, and how

they handle security issues that arise is a major issue. In particular, software companies must decide between shipping a new version of their software sooner even though it contains security bugs or delaying the ship date to address these defects. Shipping sooner can have a direct bearing upon the projected revenue from the new product, but failing to address bugs can negatively affect the company's brand image if something goes wrong.

Ongoing involvement of the executive staff is an important consideration for your information security program. Having active involvement of the executive staff can improve the likelihood of the program's success, but this will divert some time and attention from other activities. Depending too little on the executive staff can result in them pushing the program too far down in the organization. This will have the opposite effect and set up the program to fail.

The level of investment is another important consideration because many programs need to compete for limited resources within a given company. If your company considers information security of strategic importance, it must allocate the necessary funds to ensure that the program is successful. If the company decides that information security is a core competency, it must spend the necessary time and money to build an in-house team. On the other hand, it might be more appropriate to rely upon expert third parties to provide this service.

As you continue to add and improve security, keep in mind that 100 percent security is not a realistic goal. The pervasiveness of security threats, the broad diversity of enterprise networks, and the ingenuity of hackers contribute to this fact. Successful security is more about ceaselessly implementing incremental measures that reduce overall risk. Of course, you must always balance security against other business needs of the enterprise.

The following are examples of broad objectives that your company might develop.

Information Security Guiding Principles

1. We will use comprehensive architectural planning to ensure that all elements of the information security program are defined and planned.

2. We will design information security solutions for global operations from the outset, rather than local solutions that are enhanced for "international idiosyncrasies."
3. The executive staff owns information security, and it is responsible for approval of policies and oversight of the program.
4. We will treat our customer's data with the highest level of confidentiality and not share this information with third parties without customer permission.
5. We will not implement a new system that will harm our customers by disclosing their confidential information to unauthorized parties.
6. We will comply with all industry and governmental security regulations 30 days prior to required deadlines.
7. We will carefully balance the business need to quickly offer new products and services against the security risks it might pose to our customers or damage to our company brand.
8. We will adopt proven leading-edge information security technologies that will protect our company and customers.
9. We will identify internal information security core competencies to address essential value-added activities and outsource all other information security activities.
10. We will invest in information security at or above industry benchmarks for our business.

Upon completion of your strategic objectives, you are in a position to leverage this work when developing your future information security program and guiding the daily operation of the program. Your objectives should not change dramatically over time, and you should evaluate key decisions and align them with the overall goals of the program.

Business Environment

Every company has a set of unique criteria that determines how it conducts business, and your information security program should support your company's business environment. Company size, complexity, and industry are a few of the criteria that you need to consider when developing your program.

Scale your information security program to the size of your company. A smaller company, where the staff performs multiple functions, might not have a formal information security department or a CISO. In fact, a single individual might perform all the information technology and information security functions of the company.

On the other hand, a larger company that does a significant portion of its business electronically might need to have a CISO. Because disruptions to online systems can have significant impacts to the business, a more formal information security organization can prove to be an advantage.

You also need to scale security processes to the size and complexity of your organization. A smaller company might be able to operate effectively with a few informal policies. When companies expand into multiple offices and geographies, the need for formal policies becomes much more important.

Finally, the industry that your company is serving can determine the importance and scope of your information security program. Financial services industries require higher security due to the potential effect that fraud can have on their business. The health care industry also has high standards for security. Federal regulations require that health care providers protect sensitive personal medical information. In contrast, many small businesses that do not rely heavily on computer systems will not require an extensive information security program.

Table 3-1 provides some criteria that you can use to determine the importance of information security at your company. Using a simple method of 3 for high, 2 for medium, and 1 for low, you can grade your company's dependency upon information security. Note: These forms are provided in Appendix A, "Security Evaluation Framework," which you can photocopy and use at your organization.

Table 3-1

Information Security Business Dependency Matrix

Component	Ratings (High - 3, Medium - 2, Low - 1)
Company Characteristics	
■ Dependence upon systems to offer products and services to customers	
■ Value of company's intellectual property stored in electronic form	
■ Requirement for 24-7 business systems	
■ Degree of change within company (expansions, M&A, new markets)	
■ Business size (number of offices, number of customers, level of revenue) and complexity (processes, systems, products)	
Industry Characteristics	
■ Budget for security administration and security initiatives	
■ Potential impact to national or critical infrastructure	
■ Customer sensitivity to security and privacy	
■ Level of industry regulation regarding security (GLBA, HIPAA)	
■ Brand or revenue impact of security incident	
■ Extent of business operations dependent upon third parties (partners, suppliers)	
■ Customers' ability to quickly switch vendors based upon their ability to offer services in a secure manner	
Average Overall Ranking (Total Scores/12)	

By using this simple ranking, you can obtain a general idea of your company's dependence upon information security. Because no two companies are the same, you can modify this table to evaluate your entire business or to examine specific parts. If you find that your company is highly dependent

upon information security, the remaining portions of this book contain detailed suggestions for a comprehensive review and improvement of your program.

If your company has a low ranking, you might want to be more selective in your review and improvement plans because you might not want to devote many resources to security at this point. However, you will want to revisit this analysis on a periodic basis as your company expands and offers new products and services. Your business might become more reliant upon information systems and might need an information security program in place to protect these systems in the future.

Tactical Issues

Although it is important to take a long-term view of your information security program and develop a solid strategy, you might need to address some immediate issues. This can include tactical issues that your company is facing due to either industry requirements or government regulations. As we have mentioned, the health care and financial services industries have some specific requirements that they need to address to conduct business.

On the other hand, you might have recently been hacked and might need to address customer concerns regarding your handling of confidential information. Of course, this takes precedence over all other activities. Regardless of the nature of the issue, you need to do something before you are able to complete your future strategy.

Developing a *90-day tactical plan* is an effective way of addressing these issues while you're completing your strategy. Ninety days is enough time to complete the analysis necessary to develop your information security strategy and to begin remediation of any tactical issues. At this point, you should resist the natural urge to go completely into tactical mode. Address some of the most serious issues; however; you need to balance this against the strategic goals for the organization.

Key objectives for the 90-day tactical plan include the following:

- High-visibility issues that need to be addressed now
- Critical decisions that cannot be postponed

- Quick wins that can be accomplished, garnering support for the information security program
- Defer major architectural decisions and large expenditures until the overall information security strategy has been developed

The plan sends a message to your organization that you are aware of the key issues and have plans to address them now. It also provides an opportunity to improve the rapport with members of the organization who might not be pleased with your current information security organization while showing that you can make a difference.

In the initial discussions about the information security program, it is important to understand the business strategy, along with existing pain points. Look for *quick wins* that you can accomplish during the first 90 days that will help you win support for strategic initiatives that will be more difficult to accomplish. It is also important to identify or create *business champions* of the new information security initiatives. The enthusiasm of these early supporters will drive the funding and implementation process.

During the first 90 days, it is important to *over-communicate* whenever possible, including both good and bad news. Spend a great deal of time with the key managers and the information security staff to understand the situation before drawing any conclusions. One technique that can be effective is to develop a consistent status report to communicate the progress during the first 90 days. Monitor critical information such as the project objectives, recent results, and upcoming milestones and address progress on key issues that management has identified. By following this approach, you can communicate using a common methodology and minimize any misunderstandings regarding the information security program.

Your 90-day plan will be successful if you can accomplish the following:

- Address some of the current pain points in the organization
- Establish a rapport with key organizations that are affected by this program

- Set up a consistent mechanism for tracking the status of projects
- Avoid the urge to make major architectural decisions until you have conducted adequate research

Remember, no two companies are the same, and you will need to customize your tactical activities, just as you did with your strategic activities. The key point is to make an immediate improvement to the organization while you are developing your strategic plan. The organization will probably not remember what occurred during the 90-day period but rather that you addressed some key issues and developed a strategy.

Business Requirements Summary

The result of this analysis needs to be a broad range of strategies that you can use to develop some achievable objectives for the next few years. These objectives must be broad enough to guide the information security program and provide the organization with a specific roadmap for implementation. For example, a company in the health care industry might have a broad objective of staying in compliance with HIPPA regulations and offering online access to critical medical information to their customers within the next six months. This is an example of broad boundaries that will help to guide deliverables for the information security program.

Objectives will vary considerably between companies and will serve as the overriding principles for an information security program. Company size, complexity, and line of business are a few examples of criteria that will drive the appropriate information security program for your business. Compare any activity that you pursue to these objectives to ensure that you are in alignment. Always tailor your information security program to meet your company's requirements; doing the opposite is the surest route to failure.

After completing your business requirements analysis, you are in a position to proceed with the second step of the methodology, which evaluates your current information security program and designs your future desired program. This step is divided into the three key program components: people, processes, and technology. The next three chapters address each component in turn.

Developing Your Information Security Program Summary

This chapter introduced the information security life cycle and reviewed a methodology that can be used to develop an information security program for your organization in approximately 90 days. The methodology begins with establishing the current state of your program, commonly called your "baseline," and provides the steps required to develop a plan to reach your desired future state. We followed the first step of the methodology and reviewed the steps necessary to complete the business requirements analysis portion of your information security program.

Key Points for This Chapter

- A structured methodology should be used when developing your information security program.
- The first step in this process is to determine the business objectives that you want to accomplish with your program, such as providing the highest protection possible for your customer's sensitive information.
- Assessing the current state of your program and determining the desired future state is the second step in the process.
- The final step includes gap analysis between your existing program and desired future program and providing alternatives to bridge this gap.
- The Security Evaluation Framework is a tool that can be used to guide this process and develop an information security roadmap in 90 days.
- The framework includes the ability to tailor your program based upon unique company and industry characteristics because no two companies are the same.